EBRC Engineering Biology Research Consortium

Strengthening a Safe and Secure Nucleic Acid Synthesis Ecosystem

Outcomes of EBRC Stakeholder Engagement

January 2025

www.ebrc.org

1900 Powell St, Suite 1200, Emeryville, CA 94608

This material is based upon work supported by the United States National Institute of Standards and Technology (NIST) under Cooperative Agreement #70NANB24H016. Any opinions, findings and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NIST.

Citation: Engineering Biology Research Consortium (2025). *Strengthening a Safe and Secure Nucleic Acid Synthesis Ecosystem: Outcomes of EBRC Stakeholder Engagement*. Engineering Biology Research Consortium. DOI: 10.25498/E4311B

Strengthening a Safe and Secure Nucleic Acid Synthesis Ecosystem

Table of Contents

Authorship and Acknowledgements

Project Leadership & Authors

Rebecca Mackelprang, PhD	EBRC Director for Security Programs
Sebastian Rivera, PhD	EBRC Science Policy Postdoctoral Fellow
Jonathan Klonowski, PhD	EBRC Science Policy Postdoctoral Fellow
Lorenzo Smith	EBRC Intern; University of Utah PhD Candidate
India Hook-Barnard, PhD	EBRC Executive Director

Acknowledgements

This report is the result of information and insights shared across six virtual workshops, a two-day in-person workshop, and many individual and small group conversations. We acknowledge and appreciate the significant time that workshop attendees dedicated to sharing their expertise.

We also acknowledge and thank the Project Planning Committee, which met regularly to provide guidance on priority workshop topics. Project Planning Committee members included: Sarah Carter (Science Policy Consulting, LLC), Craig Bartling (Battelle), James Diggans (Twist Bioscience), Nathan Hillson (Lawrence Berkeley National Laboratory), Kevin Flyangolts (Aclid), Steven Fairchild (MITRE), John Dileo (MITRE), Mariam Lekveishvili (HHS ASPR), Matthew Sharkey (HHS ASPR), Sheng Lin-Gibson (NIST), Geoffrey Taghon (NIST), and Scott Jackson (NIST).

We gratefully acknowledge our partners at NIST. The collaborative nature of this project enabled its success.

Finally, we acknowledge the EBRC staff members who contributed to this project: Emily Aurand (Director of Roadmapping; Director of Education), Garrett Dunlap (Associate Director for Policy & International Engagement), Kaitlyn Duvall (Project and Research Associate), Mary Tomagan (Senior Administrator), and Elizabeth Allen (Senior Administrator). We thank former EBRC staff member Cynthia Ni, now of BEAM Circular, for her early work to launch this project.

Acronyms & Terms

USG	United States Government
Providers	nucleic acid synthesis providers
IGSC	International Gene Synthesis Consortium
HHS	United States Department of Health and Human Services
SOC	sequence of concern
HHS Guidance	Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids
Customers	synthetic nucleic acid customers
EBRC	Engineering Biology Research Consortium
OSTP	Office of Science and Technology Policy
OSTP Framework	OSTP Framework for Nucleic Acid Synthesis Screening
NIH	National Institute of Health
Bio-ISAC	Bioeconomy Information Sharing and Analysis Center
NIST	National Institute of Standards and Technology
CSF	NIST Cybersecurity Framework
C-SCRM	Cybersecurity Supply Chain Risk Management
NCCoE	The National Cybersecurity Center of Excellence
WMD	Weapons of Mass Destruction
BSL	Biosafety Level
FSAP	Federal Select Agent Program
MFA	multi-factor authentication
IBBIS	International Biosecurity and Biosafety Initiative for Science
DIY	Do It Yourself
NGO	non-governmental organization
GO	Gene Ontology
CCL	Commerce Control List
BSAT	Biological Select Agents and Toxins
BDT	biodesign tool
FunSoCs	Function of Sequences of Concern
PathGo	Pathogenesis Gene Ontology
CCL	Commerce Control List
JHCHS	Johns Hopkins Center for Health Security
AI EO 14110	Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

Executive Summary

Nucleic acid synthesis technologies support and enable a wide array of life sciences research and the application of that research to societal challenges. Modern synthesis technologies are highly efficient. Short oligonucleotide orders can be fulfilled and delivered within 24 hours in many parts of the world, while gene-length fragments of DNA can be delivered in about a week.

However, nucleic acid synthesis providers ("Providers"), policymakers, researchers, and others have recognized that synthetic nucleic acids could be leveraged by a nefarious or careless actor to, for example, synthesize or enhance, then release, pathogens or toxins. Efforts to address such hazards were first introduced by the International Gene Synthesis Consortium (IGSC) in 2009 and by the United States Department of Health and Human Services (HHS) in 2010, which established recommendations for validating customer legitimacy and conducting sequence screening to flag orders containing sequences of concern (SOCs). More recently, in 2023, HHS released updated guidance that expanded upon the definition of a "SOC," strengthened sequence screening recommendations, and expanded best practices to additional stakeholders, including manufacturers of benchtop synthesizers. Shortly thereafter, the White House issued an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (AI EO 14110), which instructed the director of the Office of Science and Technology Policy (OSTP) to collaborate with several federal agencies to develop a framework that would "encourage providers of synthetic nucleic acid sequences to implement comprehensive, scalable, and verifiable synthetic nucleic acid procurement screening mechanisms" while establishing standards and recommending incentives. In April of 2024, OSTP fulfilled this directive, issuing the "Framework for Nucleic Acid Synthesis Screening" (OSTP Framework), which incentivizes nucleic acid screening by requiring recipients of federal funds to purchase synthetic nucleic acids only from Providers that self-attest to adhering to the Framework. The OSTP Framework outlines six actions Providers must take for adherence and self-attestation:

1. publicly attest to adherence to the framework;
2. screen orders for sequences of concern (SOCs);
3. screen Customers and ensure legitimacy of any Customer ordering a SOC;
4. report illegitimate orders;
5. retain records of orders; and
6. implement cybersecurity and information security practices.

The National Institute of Standards and Technology (NIST) was also instructed to engage with industry and relevant stakeholders to develop and support the implementation of best practices for effective nucleic acid synthesis screening, including conformity assessment best practices and mechanisms. In partial fulfillment of this directive, NIST entered into a cooperative agreement with EBRC to facilitate industry engagement through a series of workshops. EBRC held six, two-hour virtual workshops between April and August 2024, and a two-day in-person workshop in September. Nucleic acid synthesis Providers, screening Tool Developers, academic and industry researchers, policymakers, and other security / biosecurity stakeholders participated in lively, fruitful discussion. Virtual workshops generally began with one to three short talks, followed by a discussion guided by pre-developed worksheets. The in-person workshop had several sessions following that same format, in addition to more interactive small-group exercises. Participants were encouraged to participate in discussion and/or enter their thoughts and comments directly into shared worksheets. Stakeholder engagement in these workshops directly informed EBRC's development of best practices and recommendations described herein.

Mechanisms for Attestation of Conformity

The 2024 OSTP Framework directs Providers to take six actions in order to adhere to the Framework, the first of which is self-attestation. Self-attestations can be publicly posted or provided to nucleic acid synthesis Customers or federal funding agencies upon request. This communication of adherence requires: (a) a signature of authority from the

organization; (b) point of contact information; (c) an update of the attestation annually or when the point of contact changes; and (d) the Provider to notify Customers within three days if they no longer adhere to the Framework. Additional information may be provided in self-attestations. To support standardization of Provider screening practices and strengthen Provider confidence in their self-attestation, NIST has developed, with consultation from EBRC workshop participants and IGSC members, a "Standard Guide for Providers in support of self-attestation to the Framework for Nucleic Acid Synthesis screening" ("Draft Standard Guide"). The Draft Standard Guide enumerates information that Providers may collect or actions they may take to demonstrate Framework adherence. Stakeholders may continue to engage NIST on this Draft Standard Guide in the near-future to make it as useful as possible to industry. As Customers and their institutions endeavor to ensure their own adherence to the Framework and resultant federal funding requirements, a third-party hosted, publicly accessible list of Provider self-attestations, like that currently maintained by the Johns Hopkins Center for Health Security, is critical.

Best Practices

- Providers should adhere to the OSTP Framework and make their self-attestations of adherence available on their websites and via a centralized aggregation site, such as that hosted by JHCHS.
- Customers should order nucleic acids only from Providers that adhere to the OSTP Framework, especially when using federal funds.

Recommendations

- A third-party should maintain a publicly accessible list of Providers who have self-attested to adherence to the OSTP Framework, along with copies of or links to those self-attestations, which can be referenced by research institutions and Customers seeking to implement best practices (immediate and on-going).
- NIST should continue to refine its Standard Guide and, moving forward, systematically review and update the Standard Guide, while socializing it for adoption, in order to support the development of screening standards and promote harmonized screening practices (Immediate and on-going).
- Providers should, in consultation with public- and private-sector stakeholders, consider what an ideal approach to third-party verification of screening performance might look like and consider partnering with others to try different approaches (12 months).

SOC Screening

The OSTP Framework broadly defines a Sequence of Concern (SOC) as a sequence that is a Best Match to a sequence from a federally regulated agent. This paradigm is concise but does not fully reflect sequence hazard (many sequences unique to regulated agents are benign, and some hazardous sequences are not from or unique to regulated agents). The OSTP Framework and HHS Guidance encourage a shift toward risk-based definitions or criteria for identifying SOCs, although the complexities of developing a standardized approach to determining sequence hazard is a significant challenge. If successful, a "function of concern" paradigm or, eventually, a "property of concern" approach that takes not just sequence, but environmental and cellular contexts, into account, could minimize much of the uncertainty around sequence decision-making and enhance Provider defensibility of screening decisions.

The rapid development of AI-enabled biological design tools further underscores the need to build or refine capabilities for sequence screening that go beyond sequence identity / Best Match. Capabilities are advancing to enable the creation of functional sequence variants that have similar function, but low sequence homology, to traditional SOCs (synthetic homologs). Efforts should continue to understand screening systems' susceptibility or resilience to AI-generated synthetic homologs and adjust them as needed.

Nucleic acid synthesis screening tools generally rely upon databases of SOCs. Screening would likely be more consistent across Providers if their screening systems referenced the same SOC database(s). However, many challenges were identified to developing and using a centralized, common SOC database, including curation decision-making authority, funding mechanisms, and responsibility for database maintenance. Furthermore, stakeholders held

conflicting viewpoints as to the tradeoff between security and accessibility of such databases—particularly when they contain sequences beyond federally regulated agents.

Providers currently have no means to measure the performance of their screening systems. Providers and screening Tool Developers supported the development of various test sets to assess their conformity to requirements such as those in the OSTP Framework. They also discussed the value of benchmarking test sets for better understanding industry-wide sequence designations, which may support discussion and improved screening across the board. Of course, such test sets must be developed, administered, and maintained. As directed by AI EO 14110, NIST developed an "attestation" test set, which will be made available to Providers to enable them to confirm, via an independent third-party, that their screening practices are sufficient for self-attestation.

Best Practices

- Creators of SOC databases and test sets should take measures to secure potential information hazards and ensure that these resources are continually updated. Providers and Tool Developers should continually evaluate their screening tools and systems.
  - Developers and managers of Sequence of Concern databases should consider database content and intended users in determining appropriate database security measures and access controls. Databases that contain unencrypted sequences from new and emerging threats, certain sequence variants, and/or SOCs from unregulated agents should implement enhanced security practices.
  - Developers and managers of Sequence of Concern database(s) should have documented and funded plans for improving and maintaining such databases by filling existing gaps and incorporating new research as the biothreat landscape changes.
  - Tool Developers and Providers should, potentially with the assistance of third parties, periodically assess the performance of their tools and sequence screening systems against AI-generated sequence variants that are likely to have conserved function but lack high sequence homology. As possible, patches to AI vulnerabilities should be developed and applied by Tool Developers and/or Providers.
  - When available, Providers should participate in conformity assessments to ensure their screening practices meet relevant standards, such as that set by the OSTP Framework.

Recommendations

- NIST and HHS, along with other relevant stakeholders across USG, should continue to engage with Providers and Tool Developers to develop a more robust conceptualization of "Sequence of Concern," to develop and improve screening assessment mechanisms, and to identify new threats that may be mitigated by nucleic acid synthesis screening.
  - To prioritize sequence screening resources on sequences that pose the greatest concern, the US Government should fund and/or encourage an enduring and dedicated public-private effort to develop a process for determining whether or not a sequence is "of concern" and its level of risk (6–24 months).
  - Congress should direct NIST to continue its engagement with industry to support the development of conformity assessment schemes and standards for nucleic acid synthesis screening (3-48 months).
  - USG should continue to support the development of guidance and standards for nucleic acid synthesis screening (on-going).
- Providers should identify and engage with third-parties, like IBBIS and USG entities, to enable independent verification of screening best practices and monitor emerging dual-use technologies like AI/ML-enabled Biodesign Tools.
  - A third party, trusted by public and private stakeholders, should administer conformity assessments for the nucleic acid synthesis industry (3-12 months).

- Private-sector organization(s) should develop benchmarking evaluations of nucleic acid synthesis screening systems to identify points of divergence between Providers and enable conversation and analysis that supports improved screening industry-wide (6–12 months).
- The NIST AI Safety Institute should work with industry to support regular assessment of the resilience of screening tools to synthetic homolog sequences designed by state-of-the-art Biodesign Tools (indefinite).
- Providers and/or Tool Developers should regularly test the resilience of their screening systems and tools to AI-designed sequences of concern (indefinite).

Customer Screening

Providers may collect customer information at the time of account creation, at the time an order is placed, and during follow-up screening of flagged orders. Customer identity should be confirmed or verified for each order, while Customer legitimacy should be confirmed for orders containing SOCs. Customer identity can first be validated at the time of customer account creation, e.g., through phone number or email verification. Additionally, when an order is placed, Providers should require Customers to provide, at minimum, their name, institution or affiliation, address, phone number, and email. Given the volume of orders some Providers receive, identity verification must be automated to be feasible for each order. When a Provider identifies that an order contains a SOC through sequence screening and/or Customer disclosure, the Provider should verify the legitimacy of the Customer. USG and members of the private sector have worked to develop guides for the types of information that may sufficiently verify customer legitimacy. However, this remains challenging as the information provided by Customers to demonstrate legitimacy can vary significantly in quality and detail. In the future, it may be appropriate for NIST to work with key stakeholders to develop a matrix to determine the amount of evidence needed from Customers for different tiers of SOCs. Providers may also consider utilizing third party services to alleviate the burden of Customer screening. Such options may include incorporating Customer screening within the sequence screening process, involving biosafety professionals (or other relevant personnel) from the Customer's institution during the ordering process, or creating a pre-authorization process that provides a trusted Customer with a certificate for ordering certain types of SOCs.

Best Practices

- Providers should strive to verify Customer identity for every order, and in the case of SOC orders, strive to implement screening practices and information collection that ensures Customers seeking SOCs have a legitimate, safe, and peaceful purpose for those SOCs.
  - Providers should collect information from each Customer including, minimally, name, affiliation, address, phone number, and email, and should ask Customers if their order contains a SOC when submitting orders.
  - Providers should implement reasonable mechanisms to verify the identity of Customers (regardless of whether or not they are ordering SOCs). Such verification could include automated email verification or a mechanism to confirm that shipping addresses match given institutions.
  - When a Customer orders a SOC, Providers should verify Customer and Institutional legitimacy before fulfilling the order.
  - When Customer legitimacy cannot be verified for orders containing SOCs, Providers should decline to fulfill the order.

Recommendations

- USG should fund an entity, such as NIST, to continue engaging with Providers, biosecurity experts, and other relevant stakeholders to synthesize robust methods for performing risk assessments on SOC orders.
  - A government entity such as NIST should engage Providers, academics, and biosecurity experts to matrix SOC tiers against needed evidence for the demonstration of Customer legitimacy (12–36 months).
  - NIST should continue to engage with Providers and other stakeholders to develop and encourage the adoption of standards for verifying Customer identity and Customer legitimacy (6–12 months).

- Providers should pursue new methods for establishing Customer identity and legitimacy, including engaging third parties on new security technologies.
  - Providers should implement systems to confirm Customer identity through multiple factors like email or phone number verification at the time of account creation (6–12 months).
  - USG or another funder should fund an analysis of third-party Customer legitimacy verification options (6–18 months).

Law Enforcement Reporting

Providers who receive suspicious purchase orders are encouraged to report those orders to law enforcement, specifically local FBI Weapons of Mass Destruction (WMD) Coordinators, per HHS Guidance and the OSTP Framework. The FBI has made itself available to Providers, and the HHS Guidance and OSTP Framework encourage Providers to establish and maintain relationships with their local FBI WMD Coordinator(s). These relationships facilitate the communication of emerging concerns. Anecdotally, Provider reporting practices vary widely. Industry, NIST, or other stakeholders could consider developing decision-making support guides that include support for FBI reporting decision-making.

Best Practices

- Providers should work with their local FBI WMD Coordinator to relay concerning orders and perform risk assessment.
  - Providers should identify their local FBI WMD Coordinator and establish a working relationship.
  - When a Provider is uncertain about reporting an order, the Provider should consider reaching out to local FBI WMD Coordinators to assist in decision making, even if they choose not to disclose the Customer name.
  - Providers should report highly suspicious orders for SOCs to local FBI WMD Coordinators or other relevant law enforcement officials.

Recommendations

- NIST should work with industry to further develop and/or support the development of Customer screening guides that include decision-making support for FBI reporting (12 months).

Record Retention

Retained records are important i) in the event of an investigation following an attempt or execution of a bio-related crime; ii) for detecting SOCs split across orders to a single Provider; and iii) for demonstrating Provider due diligence. In the future, records could be used for auditing purposes or for detecting SOCs split across orders to different Providers. HHS Guidance and the OSTP Framework state that Providers should maintain customer and respective order information for at least three years. To standardize recordkeeping, it is recommended that NIST engage with Industry and key stakeholders on an on-going basis to refine its draft Standard Guide, which can be used to determine which information fields are important to retain.

Best Practices

- Providers should record and retain Customer information and order information for at least three years.

Recommendations

- NIST should continue to engage stakeholders on its Standard Guide, and as it is finalized, determine in partnership with industry which information fields should be retained (6–12 months).

Cybersecurity and Information Security

The OSTP Framework encourages Providers to be diligent to ensure cybersecurity and information security. Most critically, SOC databases should be appropriately secured to prevent an informational hazard – especially for databases with SOCs beyond those from regulated agents. Several key NIST publications may guide Providers in implementing cybersecurity and information security practices.

Best Practices

- Ensure that SOC databases are implemented with proportional cybersecurity risk management strategies based on their content. Databases containing easily accessible, publicly available sequences from regulated agents and organisms may require less security than expanded databases and/or databases that describe the functions of sequences that may not be widely known to be concerning.

Recommendations

- NIST should engage Providers and government stakeholders on the development of a CSF 2.0 Community Profile for Providers (1–2 years).

Education and Implementation Support

Informational outreach and socialization of the HHS Guidance, OSTP Framework, and associated federal awardee requirements is necessary to achieve compliance by all relevant stakeholders. Stakeholders such as academic research Customers may be unaware or confused by new policies and practices. For this reason, stakeholders who are aware of them should continue to socialize new requirements and provide helpful resources.

Best Practices

- Providers, along with research institutions, should ensure that the OSTP Framework, HHS Guidance, and updated NIH funding requirements are properly socialized to Customers and awardees.
  - Providers and other members of industry should socialize U.S. nucleic acid synthesis screening policies with their Customers to spread awareness and encourage implementation.
  - Industry and other stakeholders should coordinate efforts to educate researchers and other potential Customers of nucleic acids of all nucleic acid procurement requirements for federal fundees.
  - Institutions should support the research community in understanding Provider self-attestation and in purchasing nucleic acids from attesting Providers.

Recommendations

- OSTP and/or federal funding agencies should clarify how the OSTP Framework applies to Customers with mixed funding or with awards granted prior to implementation of the Framework (6 months).
- Federal funding agencies that implement the OSTP Framework should outline consequences for awardees of federal grants who are out of compliance (6 months).

Introduction

In the last twenty years, the capabilities of the nucleic acid synthesis industry have grown while production costs have come down, making synthetic gene fragments, synthetic genes, and even synthetic genomes, readily available to the research community. This access to longer, higher-fidelity genetic sequences facilitates scientific progress, enabling researchers to answer research questions more quickly and work toward solutions to pressing application challenges. However, these expanded capabilities also raise significant dual-use concerns. Customers could attempt to order nucleic acids that could be used to, for example, recreate, spread, or intensify pathogens, toxins, or illicit substances. As nucleic acid synthesis continues to become faster and less expensive, and as accompanying biological research tools develop in parallel, appropriate safeguards are needed to ensure the progress of beneficial research while minimizing associated risk.*

One important safeguard is the screening of synthetic nucleic acids orders. Screening involves assessing how hazardous a given sequence may be and ensuring that the individual and/or organization ordering the sequence is poised to responsibly use it. Screening is challenging, however, and screening practices across the synthesis industry vary. Stakeholders in government, industry, and non-governmental organizations have all taken crucial steps to support, enable, and encourage screening. This report reflects the effort of a public-private partnership to convene these stakeholders to identify and address on-going screening challenges, alongside forecasting needs and opportunities for improved screening practice and implementation in the future.

This work builds upon nearly two decades of dedication to safe and secure nucleic acid synthesis from members of industry, the U.S. Government (USG), and others. In 2009, the five nucleic acid synthesis providers ("Providers") representing the majority of gene synthesis capacity at that time formed the International Gene Synthesis Consortium (IGSC).[1] The IGSC issued its first "Harmonized Screening Protocol for Gene Sequence & Customer Screening to Promote Biosecurity" in 2009.[2] In parallel, the United States Department of Health and Human Services (HHS) developed the "Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA," published in 2010.[3] Both of these resources recommended that Providers screen their customers and both develop and conduct sequence screening to identify orders containing "sequences of concern" (SOCs).

The 2010 HHS guidance remained in place until October 2023, when HHS issued its updated "Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids" ("HHS Guidance").[4] The updated Guidance is largely consistent with the original, but includes key changes that reflect expanding capabilities of Providers and their customers ("Customers"). More specifically, it:

- recommends that, as soon as it is practical to do so, industry expand its definition of SOCs beyond sequences from regulated agents;
- narrows the recommended sequence screening window from 200 to 50 nucleotides;
- includes best practices for additional stakeholders, including Customers, Principal Users, and End Users of synthetic nucleic acids, such as:
  - preemptively providing information that demonstrates legitimacy when ordering a SOC;
  - transferring synthetic nucleic acids containing SOCs only to verified individuals with a legitimate use;
  - maintaining records of transfers of SOCs to other parties and communicating transfers to biosafety officers or equivalent responsible parties;
- includes best practices for manufacturers of benchtop synthesis instruments, such as:
  - validating the legitimacy of Customers purchasing benchtop equipment to ensure the equipment is appropriate for Customer needs;
  - screening Customers purchasing benchtop synthesizer sole-use reagents;
  - implementing mechanisms to track users and sequences produced on equipment;

* Herein, we use "risk" to refer to the likelihood of a harm or consequence from a given hazard.

- integrating sequence screening capabilities into benchtop synthesis machines;
- building user authentication into the synthesizer user interface; and
- implementing mechanisms to prevent circumvention of the SOC screening methodology through physical or logical manipulation of the devices or reagents.

Just weeks later, the White House released the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (AI EO 14110), which paid significant attention to nucleic acid synthesis.[5] Under §4.4(b)(i) of AI EO 14110, the Director of the Office of Science and Technology Policy (OSTP) was directed, in collaboration with the Secretary of State, Secretary of Defense, Attorney General, Secretary of Commerce, Secretary of HHS, Secretary of Energy, Secretary of Homeland Security, and the Director of National Intelligence, to develop a framework that would "encourage providers of synthetic nucleic acid sequences to implement comprehensive, scalable, and verifiable synthetic nucleic acid procurement screening mechanism, including standards and recommended incentives."

In April 2024, OSTP fulfilled this mandate, issuing its "Framework for Nucleic Acid Synthesis Screening" (OSTP Framework).[6] Critically, the OSTP Framework marked the introduction of a mechanism to incentivize nucleic acid synthesis screening by requiring recipients of federal funds to purchase synthetic nucleic acids from Providers that self-attest to adhering to the Framework. The Framework outlines six actions Providers must take for adherence and self-attestation:

1. publicly attest to adherence to the framework;
2. screen orders for sequences of concern (SOCs);
3. screen Customers and ensure legitimacy of any Customer ordering a SOC;
4. report illegitimate orders;
5. retain records of orders; and
6. implement cybersecurity and information security practices.

As an integral part of promoting stakeholder buy-in and an acceleration of technical screening capabilities, AI EO 14110 also directed NIST, in §4.4(b)(ii), to "initiate an effort to engage with industry and relevant stakeholders" on the development and implementation of best practices for effective screening and conformity assessment for screening systems. NIST entered into a Cooperative Agreement with EBRC to facilitate this engagement, and EBRC hosted six virtual workshops ("EBRC/NIST workshops"), each two hours in duration, between April and August 2024, on relevant topics (Agendas in Annex I). Stakeholders including Providers, Tool Developers, policymakers, researchers, and other security and biosecurity professionals participated in workshops. Workshop topics, agendas, and speakers were decided in partnership with NIST and under the advisement of a Project Planning Committee.[†] The virtual workshops informed and culminated in an in-person, two-day workshop held in September 2024 in Bethesda, Maryland (Agenda in Annex II).

The first virtual workshop sought to introduce the project objectives to stakeholders and discuss two of the screening topics enumerated in AI EO 14110: best practices for the development and use of SOC databases and mechanisms for screening conformity assessment. Screening processes generally work to identify an ordered sequence, then determine if that sequence is a SOC. Thus, databases are needed to contain the sequences that are actually of concern. Such databases pose a clear information hazard if not adequately secured. However, there have not previously been mechanisms to assess if screening systems and their SOC databases perform adequately. We

[†] Project Planning Committee members included: Sarah Carter (Science Policy Consulting, LLC), Craig Bartling (Battelle), James Diggans (Twist Bioscience), Nathan Hillson (Lawrence Berkeley National Laboratory), Kevin Flyangolts (Aclid), Steven Fairchild (MITRE), John Dileo (MITRE), Mariam Lekveishvili (HHS ASPR), Matthew Sharkey (HHS ASPR), Sheng Lin-Gibson (NIST), Geoffrey Taghon (NIST), Scott Jackson (NIST), Becky Mackelprang (EBRC), Sebastian Rivera (EBRC), and India Hook-Barnard (EBRC).

therefore discussed what kinds of sequence test sets could be developed and used to assess or evaluate screening processes and SOC database composition.

These topics were expounded upon in future workshops, with the discussion of SOC database construction and management turning to discussion of database content. Even in the context of sequences from federally regulated agents and organisms, determining precisely which sequences are and are not of concern is a significant challenge. One virtual workshop considered best practices for screening Customers and for considering a sequence's level of concern in the context of a given Customer.

The final, in-person workshop sought to tie together the virtual workshop topics, refining potential best practices and forefronting the implementation of all aspects of screening, including record retention, law enforcement reporting, cyber- and information security, and screening resilience to AI-designed sequences.

This report reflects the discussions within these workshops, in addition to other engagement with relevant individuals and groups. Importantly, technology and capabilities are changing rapidly (e.g., advances in artificial intelligence and machine learning), and stakeholders are interested in moving beyond the current paradigm that defines sequences of concern solely by taxonomic group.

Furthermore, specific technical elements of the OSTP Framework are set to change in 2026—for example the definition of Sequence of Concern will expand to "include sequences known to contribute to pathogenicity or toxicity, even when not derived from or encoding regulated biological agents." As such, EBRC-led discussions sought to consider not only the immediate actions required for adherence to the Framework, but also needs for better screening moving forward. AI EO 14110 was rescinded on January 20, 2025, and it is not understood how the forthcoming OSTP will uphold the Framework, and/or if OSTP will designate an interagency group to make updates to the Framework. Some funding agencies, such as NIH, have already notified the public that "funds may only be used to procure synthetic nucleic acids or benchtop nucleic acid synthesis equipment from sources adhering to the OSTP Framework for Nucleic Acid Synthesis Screening."[7]

While we await the new Administration's engagement with this topic, stakeholders can continue to build upon existing momentum toward the implementation of self-attestation of screening practices, including SOC screening, Customer screening, follow-up screening and reporting, record retention, and cyber and information security. In this report, we discuss central issues and perspectives surrounding each of these practices, in addition to considerations for the broader community such as Customer education and outreach. Best practices and recommendations are then provided at the end of each section. Best Practices describe actions, policies, and processes that stakeholders such as Providers, Customers, and Tool Developers can implement now in support of robust nucleic acid synthesis screening. Recommendations aim to highlight pathways for facilitating the further development of best practices and key underlying capabilities and infrastructure and give a time frame during which the recommended activities should occur.

References

1. International Gene Synthesis Consortium (IGSC). *World's Top Gene Synthesis Companies Establish Tough Biosecurity Screening Protocol.* IGSC. 2009. https://genesynthesisconsortium.org/wp-content/uploads/IGSC-Launch-Announcement.pdf
2. International Gene Synthesis Consortium (IGSC). *Harmonized Screening Protocol - Gene Sequence & Customer Screening to Promote Biosecurity.* IGSC. 2009. https://genesynthesisconsortium.org/wp-content/uploads/IGSC-Harmonized-Screening-Protocol-11_18_09.pdf
3. United States Department of Health and Human Services. *Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA.* U.S. HHS. 2011;30(2):243-257, Biotechnology Law Report. doi:10.1089/blr.2011.9969
4. United States Department of Health and Human Services Administration for Strategic Preparedness and Response. S*creening Framework Guidance for Providers and Users of Synthetic Nucleic Acids.* U.S. HHS. 2023. https://aspr.hhs.gov/legal/synna/Documents/SynNA-Guidance-2023.pdf
5. The White House. *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.* The White House. 2023. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/
6. United States National Science and Technology Council, Fast Track Action Committee on Synthetic Nucleic Acid Procurement Screening. *Framework for Nucleic Acid Synthesis Screening*. U.S. NSTC. 2024. https://aspr.hhs.gov/S3/Documents/OSTP-Nucleic-Acid-Synthesis-Screening-Framework-508.pdf
7. National Institute of Health (NIH). *Notification of NIH Requirements Regarding Procurement of Synthetic Nucleic Acids and Benchtop Nucleic Acid Synthesis Equipment.* NIH. 2024. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-012.html

Mechanisms for Attestation of Conformity

The implementation of screening guidance and recommendations can be challenging. Companies have lacked any mechanism for evaluating the screening processes they implement. Anecdotally, some Providers have hired private teams to evaluate their sequence screening capabilities, thus the development of options and opportunities for standards and mechanisms for consistent screening of Customers and sequences would be welcome by at least a segment of the nucleic acid synthesis industry. The OSTP Framework noted work being undertaken by NIST to develop "conformity-assessment best practices and mechanisms." Conformity assessment could be used to evaluate the entire screening process, or to evaluate specific parts of it. Significant time in EBRC workshops was spent discussing conformity assessment for nucleic acid sequence screening.

More broadly, conformity assessment can be thought of as the process a Provider goes through before self-attesting to adherence to the OSTP Framework. As defined in NIST SP 2000-01,[1] conformity assessment:

> *provide[s] a means of assuring that the products, services, or systems produced or operated have the required characteristics, and that these characteristics are consistent from product to product, service to service, or system to system.*

NIST defines four key elements of conformity assessment: requirement, determination, attestation, and surveillance (Fig. 1). Applying these concepts to nucleic acid synthesis, the OSTP Framework lays out the *requirements*, or standards, that Providers should meet. There are six required actions for adherence to the Framework, which includes screening purchase orders for SOCs. The requirements or standards can then be used to develop tests, inspections, or audits that *determine* whether the defined requirements have been met (see *Test Sets* subsection of **SOC Screening**). Determination answers the question "How do we know the system or process performs well enough to meet the requirements?" *Attestation* ascribes the individual, organization, or institution that is declaring or documenting whether the requirements (in this case, as laid out by the OSTP framework), have been met. The Framework directs Providers to *self-attest* to their adherence to the actions described therein.

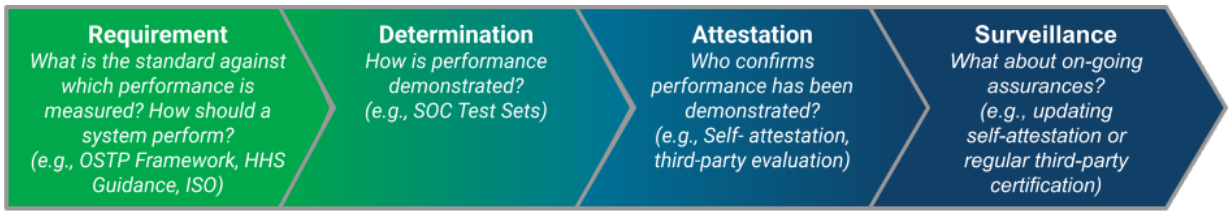

Figure 1 (*adapted from NIST SP 2000-01*[9])**:** Conformity assessment of a product, service, or system includes i) articulation of requirement(s) or standard(s) that must be met; ii) a mechanism for determining whether or not those requirement(s) are met; iii) a mechanism for communicating a product, service, or system's performance relative to requirement(s); and iv) a mechanism to regularly determine if requirement(s) are met moving into the future.

While self-attestation lacks external third-party verification, it remains an important approach to conformity assessment. In the future, it may become feasible to implement forms of third-party determination and attestation of a Provider's screening processes, for example through independent audits or systems stress testing.

Finally, *surveillance* involves ensuring that requirements are satisfied and maintained on an ongoing basis. The OSTP Framework suggests that Providers should make their self-attestations readily available and update their self-attestation annually to demonstrate their continued compliance. If conformity determination and attestation become supported by third-party(s) in the future, such third-party(s) could also provide ongoing surveillance.

In this section, we discuss the implementation of—and best practices for—the self-attestation scheme of the OSTP Framework. EBRC engaged industry and other stakeholders on the types of information that may be useful in a self-

attestation, when or if attestations need to be renewed, how they can best be communicated to stakeholders (such as Customers), and approaches to third-party conformity assessments.

Central Issues and Perspectives

Self-Attestation Templates

Different versions and ideas for self-attestation format and content were discussed and shared over the course of workshops. Shortly after the conclusion of EBRC's series of workshops, OSTP updated the Framework with a few, very useful clarifications, adding that attestations from Providers and Manufacturers require: (a) a signature from an individual of authority on behalf of the organization; (b) point of contact information; (c) a yearly update to the attestation by January 1st of each year and whenever point-of-contact information changes; and (d) an expressed commitment that federally-funded Customers and funding agencies will be notified within 72 hours if they no longer adhere to the framework.

Of course, Providers have the option to provide more detail in their self-attestations. For instance, the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 17050-1:2004 Conformity assessment - Supplier's declaration of conformity, lays out a more detailed approach to attestation. Based on this, NIST led the development a "Standard Guide for Providers in support of self-attestation to the Framework for Nucleic Acid Synthesis screening" ("Draft Standard Guide;" see Annex III) with EBRC, the International Gene Synthesis Consortium (IGSC), and the input from many stakeholders, including workshop attendees, to "support harmonized self-attestation documentation." Five "Declarations Statements" are listed, in alignment with the actions described in the Framework to which Providers should attest. Subsequently, the Draft Standard Guide provides a template that Providers may adopt in support of these declarations. This Guide should be useful to Providers in the short-term, and could lay the groundwork for greater standardization of screening practices. This template has not yet been finalized, but contains sections for:

1. Documenting self-attestation status;
2. Collecting basic Customer information and information for Customers ordering SOCs;
3. Customer identity verification;
4. Sequence screening and confirming Customer legitimacy;
5. Reporting orders to law enforcement;
6. Ensuring cybersecurity and information security[2,3]; and
7. Record retention.

In addition to moving toward consistent, robust screening, standardized information gathering and Provider practices can improve Provider defensibility to Customers unhappy with routine questions.

Compiling and Hosting Self-Attestation Forms

Stakeholders agreed that the Customer community would be well-served by the development of a centralized repository(s) of Provider self-attestations. Such a resource would enable Customers to quickly confirm that a given Provider has attested to screening. Such a resource would also be of value to research organizations working to ensure that their scientists comply with funder requirements for the procurement of synthetic nucleic acids. Thus, stakeholders discussed which entity(s) might be best suited to host self-attestations and/or list links to self-attestations. The entity in charge of such a resource would need the capacity to host and maintain it, ensuring up-to-date information that organizations and individual Customers could trust. Research institutions may not all have this capacity, thus stakeholders suggested that a government agency such as NIST or the Department of Health and Human Services' Administration for Strategic Preparedness and Response (ASPR) might be appropriate. Government agencies, however, have limitations as to the types of activities they can assume, thus discussion shifted toward private-sector organizations such as EBRC or the Bioeconomy Information Sharing and Analysis Center (BIO-ISAC). In early September 2024, the Johns Hopkins Center for Health Security (JHCHS) launched the "Gene Synthesis Screening Information Hub," a website to support stakeholders as they work to understand and implement US nucleic acid

synthesis screening policies.[4] Importantly, the JHCHS website has a list of links to self-attestations posted by companies on their own websites. Assuming it is maintained, this should be a very useful resource. As of December 20th, 2024, 12 self-attestations were posted by Providers from four nations on the JHCHS Gene Synthesis Screening Information Hub. Many were posted before the October 2024 OSTP Framework clarification, and as such, not all include the updated elements described therein (and referenced above). Importantly, this resource and any others developed to fulfill the same function must be kept up-to-date. If a Customer depends on such a resource to check a Provider's attestation status, but some attestations are missing, that Customer could needlessly discount a given company as a potential Provider. The resource developer such as JHCHS cannot be held responsible for tracking down each and every Provider's self-attestation, so the stakeholder community should make efforts to make the resource known to Providers.

Enforcement, verification, and liability issues surfaced around self-attestation. Is a Customer responsible for verifying that Providers screen? Can their federal funding be jeopardized if they use a Provider who falsely self-attests? Stakeholders were assured that, under the OSTP Framework, Customers are not expected to, and should not, investigate the self-attestations of Providers, and thus bear no responsibility for false attestations. Additionally, Providers encouraged the development of straightforward mechanisms they could use to internally verify their own compliance with self-attestation requirements.

Beyond Self-Attestation: Third-party verification

Self-attestation has some inherent downsides, as it can be difficult to see one's own weaknesses and objectively evaluate one's own practices. As such, movement towards third-party verification of screening practices may result in more robust screening and also help to identify areas of screening that would benefit from better-defined standards or requirements. Different industries have different approaches to third-party verification, validation, evaluation, and/or auditing. In nucleic acid synthesis screening, one approach may be to invite a third-party to look "under the hood" of a Provider's screening workflow to ensure standards are met. They might look at records to understand retention practices, rates of order flagging, outcomes of follow-up screening, and more. This approach would require significant preparation by Providers, and robust contractual agreements would need to be in place before a third-party was given access to such sensitive company (and Customer) records and information.

A less invasive approach to third-party verification, "end-to-end stress testing," does not require a third-party to access any non-public Provider documents. Instead, a third-party could place orders through normal processes and evaluate outcomes. End-to-end stress testing yields real insights as to how screening systems work in practice. Instead of testing just one piece of the screening workflow, such as sequence screening, the integrity of the process can be investigated. However, this approach can yield ambiguous results. A third-party evaluator knows only what order was placed and what the ultimate outcome was, which would preclude insight into the Provider's internal practices. For example, follow-up screening does not always require outreach to a customer. A Provider might flag an order, do additional research internally, and decide to ship it without direct customer follow-up. The flag and internal follow-up would be invisible to the third-party evaluator. However, an evaluator could use Customer profiles and sequences with a range of risk profiles to gain insight based on how Providers respond to each scenario.

At present, no agency within the US Government has the authority and capability to perform verification or evaluation of Provider screening practices. Several challenges have hindered the private sector's ability to carry out such work. Thus, at present, self-attestation is an appropriate mechanism for attestation (see Fig. 1) However, screening adoption and rigor may increase if the public- and private-sectors are able to work together to establish some sort of screening verification regime.

Best Practices

- Providers should adhere to the OSTP Framework and make their self-attestations of adherence available on their websites and via a centralized aggregation site, such as that hosted by JHCHS.
- Customers should order nucleic acids only from Providers that adhere to the OSTP Framework, especially when using federal funds.

Recommendations

- A third-party should maintain a publicly accessible list of Providers who have self-attested to adherence to the OSTP Framework, along with copies of or links to those self-attestations, which can be referenced by research institutions and Customers seeking to implement best practices (immediate and on-going).
  - Ready access to synthetic nucleic acids is crucial to the advancement of life sciences research. Thus, identifying Providers that self-attest to adherence to the Framework should not be an arduous task for Customers. Fulfillment of this recommendation enables Customers to access needed information quickly and easily. JHCHS has developed a useful and fit-for-purpose resource.[4] As long as it is able to be maintained, stakeholders can encourage use of this resource (and/or others of high quality) by Providers and Customers.
- NIST should continue to refine its Draft Standard Guide, and, after publication, systematically review and update it, while socializing it for adoption, in order to support the development of screening standards and promote harmonized screening practices (immediate and on-going).
  - As Providers consider and work toward implementing parts or all of the NIST Standard Guide, they should provide feedback and discuss work toward any needed changes for adoption and implementation. Standardized screening practices will ensure screening performance is robust and harmonized.
- Providers should, in consultation with public- and private-sector stakeholders, consider what an ideal approach to third-party verification of screening performance might look like and consider partnering with others to try different approaches (12 months).

References

1. Carnahan L, Phelps A. *ABC's of Conformity Assessment.* National Institute of Standards and Technology (NIST). 2018; NIST SP 2000-01. doi:10.6028/NIST.SP.2000-01
2. Raimondo, G., Locascio, L., National Institute of Standards and Technology (NIST). *NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)*. NIST. 2024; NIST SP 1305. doi:10.6028/NIST.SP.1305
3. National Institute of Standards and Technology (US). *NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide.* National Institute of Standards and Technology (U.S.). 2024; NIST SP 1300. doi:10.6028/NIST.SP.1300
4. *Gene Synthesis Screening Information Hub*. Accessed January 23, 2025. https://genesynthesisscreening.centerforhealthsecurity.org/

SOC Screening

Central Issues and Perspectives

EBRC workshops considered several technical elements of nucleic acid sequence screening, focusing on the key challenge of developing a precise, widely agreed upon, and implementable understanding of a "sequence of concern." Sequence screening has traditionally relied on lists of regulated taxa and toxins to identify sequences of concern. While this approach is expedient and probably sufficient for viruses, taxon identification is not always the best indicator of the appropriate level of concern for a given sequence from bacterial, fungal, and protozoal pathogens. Most sequences from nonviral regulated agents pose no hazard, whereas many sequences from unregulated agents can cause significant harm.[1,2,3] As such, EBRC workshops considered approaches for incorporating sequence or protein function into a maturing "sequence of concern" paradigm.

Screening processes generally utilize SOC databases to determine if the best match to an ordered sequence is "of concern." Therefore, the workshops also examined the structure, content, security, ownership, and accessibility of centralized or decentralized databases of SOCs that would support screening. This discussion included consideration of the roles of both USG and the private sector in developing and maintaining these databases.

Furthermore, the OSTP Framework and 2023 HHS Guidance suggest additional technical improvements to sequence screening that Providers should implement by October 2026. These include reducing screening windows to 50 nucleotides and considering "the potential for shorter nucleotide sequences to be assembled into SOCs when multiple synthetic nucleic acids are ordered in a bulk order or in multiple orders over time." These were a relatively minor point of discussion. Both were considered feasible, however the implementation of detection capabilities for shorter sequences split between orders was not considered a significant priority by some participants. Concerns were raised that 50 base pair windows would be detrimental to the emerging DNA data storage industry.

Finally, EBRC engaged stakeholders on the assessment of nucleic acid screening systems. Providers need mechanisms for assessing whether or not their systems conform to the basic requirements for adherence to the OSTP Framework. Beyond this foundational need, the industry would benefit from structured analyses of more advanced screening capabilities, such as identifying deliberately obscured sequences or determining whether or not a given ambiguous sequence should be flagged. In this context, the workshops also explored the developers, administrators, challenges, and benefits of different types of test sets.

Defining "Sequence of Concern"

The OSTP Framework defines a Sequence of Concern (SOC) as:

> *...a nucleotide sequence or its corresponding amino acid sequence that is a Best Match to a sequence of federally regulated agents (i.e., the Biological Select Agents and Toxins List (BSAT), or the Commerce Control List (CCL)), except when the sequence is also found in an unregulated organism or toxin...*

While straightforward, this definition does not completely reflect sequence hazard. Many sequences that potentially pose significant risk are excluded from this definition, while many sequences that are not innately hazardous, such as genes involved in homeostasis or primary metabolism (e.g., "housekeeping genes") that are highly conserved across pathogens and non-pathogens, are included. The October 2024 OSTP Framework clarification notes that Providers may still be adherent to the Framework if they develop a list of "exempted sequences" that technically qualify as SOCs based on the above definition, but do not contribute to pathogenicity or toxicity. Clearly, the use of taxonomy as a proxy for hazard is imperfect.

Furthermore, the OSTP Framework directs Providers to expand their definition of "SOC" by October 13, 2026 to:

> *…include sequences known to contribute to pathogenicity or toxicity, even when not derived from or encoding regulated biological agents…*

This expansion of the SOC definition highlights that there is considerable interest in developing a "sequence of concern" paradigm that incorporates sequence hazard more broadly. Both the 2023 HHS Guidance and OSTP Framework recognize this as a priority.

Thus, stakeholders at EBRC workshops discussed how "sequence of concern" could be defined or conceptualized to more accurately capture—and even stratify—the hazard and/or risk of a sequence's misuse. Different threat models, risk estimations, and priorities make it unlikely that unanimous consensus can be achieved on the risk profile of every sequence. However, individual stakeholders or stakeholder groups could establish a multi-dimensional rubric or set of parameters for adjudicating a level of concern and stratify sequences accordingly (e.g., see Fig 2). This would support the assessment of a given sequence's level of concern based on many factors. Decisions on particular sequences could vary to some degree, but stakeholders would have a common language with which to discuss and make arguments about given sequences.

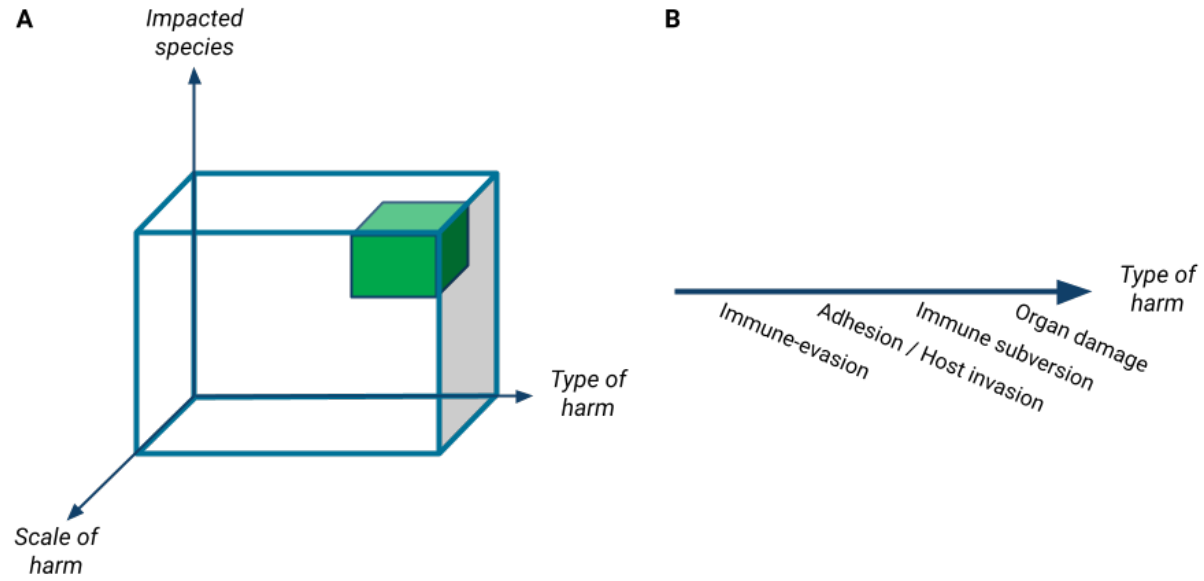

Figure 2: Example rubric for using axes to define types of sequences of greatest concern. A) Three dimensions, *type of harm*, *scale of harm*, and *impacted species* that affect the level of concern that sequences pose are shown on x-, y-, and z-axes. A given sequence could be analyzed in terms of each of these axes. For example, a sequence may be from a pathogen that subverts immune function (x), infects livestock (y), and, if misused, could threaten the food supply (z). Such a sequence would be assigned high values for each of the three axes and would thus likely end in the green "Sequence of Concern" area of the rubric. **B)** Different SOC function may confer increasing levels of harm and thus be a cause for greater concern.

Stakeholders brainstormed and considered several different dimensions or axes[4] that could be used to describe the risk associated with a sequence, including:

- *host or impacted species*: the organism(s) that a given sequence has the potential to harm (e.g., humans, livestock, staple crops);
- *type of harm*: the 2026 SOC definition in the OSTP Framework gives a high-level view of the *type of harm* that needs to be considered, citing "sequences known to contribute to pathogenicity or toxicity." Within that, the more specific function of a sequence, such as its role in the pathogenicity and/or virulence of an organism, may influence the degree to which it is "of concern." The functions of highest concern include:
  - Damage to host cells, tissues, and/or organs;
  - Subversion of innate immune signaling (e.g., via antagonism of pattern recognition receptors, or suppression of NF-κB, interferon, MAPK, inflammasome formation, etc.);
  - Subversion of innate immune effectors;
  - Enable dissemination of microbe between cells and/or tissues;

  - Enable host cell invasion; and
  - Exploit cell biological processes for microbe proliferation.

  While functions involved in the synthesis of a drug or toxin may be of concern, there was disagreement as to how they should be considered in this context. Biosynthetic enzymes for a drug or toxin may be remarkably similar to benign metabolic or housekeeping enzymes. Thus, they may trigger many false positives during screening. However, genes that code directly for a protein toxin may constitute a more significant hazard.
- *necessary/sufficient to cause harm*: a sequence could be sufficient to make an attenuated or nonvirulent organism virulent (sufficient), or, if knocked out of a pathogen, it may attenuate the pathogen (necessary). Sufficient SOCs would be of greater concern than necessary SOCs; some "necessary" sequences may not be SOCs at all if involved in basic cellular activities such as metabolism;
- *strength of the evidence*: one or more labs independently characterizing a harmful function and demonstrating the mechanism through multiple techniques is strong evidence, while one lab using transcriptomic data or transposon knock-out experiments to suggest a role in pathogenicity is *considerably* weaker evidence;
- *potential for weaponization*[‡]: the ease with which a sequence could be used deliberately as a weapon or to create a weapon;
- *potential for mitigation:* the deterrence, prevention, and response capabilities to the misuse of a sequence, e.g., a sequence for a pathogen antigen with readily available antibody therapeutics might be of less concern than one for which no treatments are available;
- *scale of harm*: as more people and/or valued species are negatively impacted, the scale of harm increases. If *scale of harm* is prioritized, sequences like those for toxins that can cause significant harm to a few individuals may be deemed less important than sequences that can be used to cause wide-scale harm;
- *biotechnology application* - some sequences (e.g., segments of the *Orthopoxvirus variola* genome) have no or very few legitimate use cases, while some sequences from concerning organisms are useful as molecular biology tools (e.g., IRES, 2A peptides) and thus are ordered frequently for legitimate uses.

After brainstorming and discussing these and other potential dimensions, stakeholders used a voting tool to rank the importance of each dimension. *Type of harm (function)* and *scale of harm* were the highest rated as dimensions for describing the level of concern caused by a sequence (Table 1). *Host or impacted species* and *potential for weaponization* were the third and fourth highest ranked, respectively.

For these dimensions to be useful, common language is needed for placing a given sequence's location along each dimension (see Fig. 2b). For example, if the level of concern of a sequence is adjudicated based on *type of harm* (function), then types of harm such as "immune subversion," "organ damage," or "cell adhesion and invasion" need to be classified by level of concern. The scientific community has engaged in a number of efforts to create standardized functional annotations, including Gene Ontology[5] (GO), Pathogenesis Gene Ontology[6] (PathGo), Function of Sequences of Concern[3] (FunSoCs) and Battelle's hazardous function database,[2] that can provide common language for describing and evaluating *type of harm*. Work continues to improve functional annotation, including by refining pathogenesis-related GO terms for integration into public databases. If functions of concern can be well-defined and ascribed to sequences, then specific functions could be identified as benchmarks of high, medium, and low concern. A given sequence's function could then be identified along the axis relative to those benchmarks. As different axes are matrixed together, a multi-dimensional "area of concern" could be drawn or calculation made to reflect how the interaction of different axes, like *type of harm, scale of harm,* and *host species*, impact the overall level of concern of a sequence. Different presenters and discussants at EBRC workshops discussed related approaches and paradigms.

[‡] For more on weaponization, see *Biodefense in the Age of Synthetic Biology* (NASEM. 2018. https://doi.org/10.17226/24890.), where "usability as a weapon" is identified as one of four key factors for assessing the level of concern posed by a capability in synthetic biology. "Production and Delivery," "Scope of Casualty," and "Predictability of Results" can each be incorporated into considerations of weaponization.

Axis	Average	Median
Scale of harm	*4.4*	*5*
Type of harm (function)	*4.3*	*5*
Host or impacted species	*3.6*	*4*
Potential for weaponization	*3.5*	*4*
Necessary/Sufficient	*3.3*	*3*
Potential for mitigation	*3.3*	*4*
Strength of evidence	*3.2*	*3*
Biotechnology application	*3.0*	*3*
Relatedness between controlled and non-controlled species	*2.6*	*3*

Table 1: Axes of greatest impact on a sequence's level of concern. EBRC workshop participants discussed the characteristics or dimensions of a sequence that might have the greatest impact on the level of concern it poses. Participants (n = 40) were asked to vote on which characteristics were most important, with a 1 indicating completely unimportant, 5 being essential, and 3 indicated that further information was needed to make a decision.

One presenter described their organization's Probabilistic Risk Assessment approach to building sequence screening capabilities, wherein a risk level for a sequence is assigned based on many sequence properties. Were this strategy to be further developed, a subset of stakeholders could gather over a few days to begin to drill down on the sequence properties with the greatest impact on sequence risk and how they might be matrixed to define a sequence's level of concern.

This matrixed approach to identifying sequences of concern may or may not be the best path forward. Individual stakeholders may prefer different technical and organization/operational approaches. The IGSC Test Set Working Group has begun building a process for determining, via Internet Engineering Task Force-style rough consensus,[7] whether or not specific categories of sequences should be flagged for human review. As the process is developed, the Working Group is also expanding the set of involved stakeholders towards a goal of fostering a broad international community of screening Tool Developers, nucleic acid Providers, regulators, pathogen experts, policy developers, security experts, and others with relevant knowledge and concerns.

A successful SOC paradigm will need a built-in, established process for making updates as new information is learned, as capabilities advance, and as the biothreat landscape changes. Particularly now, as the stakeholder community ideates on how to move beyond taxonomy-based screening, different parallel efforts should be encouraged to proceed, ideally informing one another. Different approaches may ultimately end up contributing to screening advances in different ways. However, care should be taken to avoid duplication of effort and to avoid the creation of several incompatible approaches to identifying "sequences of concern." Ultimately, the stakeholder community must pursue organized, dedicated, focused efforts to, minimally, build loose agreement around classes of sequences for which Providers should screen. In the future, as one presenter at an EBRC workshop suggested, SOC or function of concern paradigms might be superseded by a "property of concern" paradigm that incorporates system-based thinking about genomic contexts and the stochasticity and randomness that occurs within cells.

Recognizing AI-Generated Sequences of Concern

Capabilities at the intersection of AI and life sciences research have expanded greatly in recent years, enabling modeling of protein folding, functional prediction, and even protein interactions with small molecules and other proteins.[8,9,10,11] Alongside their beneficial uses, these capabilities make it possible to use AI to design variants of sequences of concern that have wild-type function with low homology to wild-type sequences (synthetic homologs). Such sequences could potentially bypass sequence screening systems, which commonly rely on some form of sequence similarity.

However, current AI-enabled biodesign tools (BDTs) are imperfect. Researchers may still need to test several AI-designed synthetic homologs before finding one that is equivalent to or superior to wildtype. One workshop presenter reviewed literature precedent for enzyme design using BDTs and found that designed enzyme success rate decreased significantly as sequence identity to wild-type sequences decreased. This further highlights the current limitations of BDTs for creating potentially hazardous proteins that would avoid detection by homology-based sequence screening. Biodesign capabilities continue to advance, and so in the future, identifying the best synthetic homologs may require less experimental work. It is therefore critical that screening systems be made resilient to AI-enabled sequence obfuscation.

A new study highlights that sequence screening tools are—or can be patched to be—able to detect synthetic homologs.[12] The authors used available BDTs to generate variants of sequences of concern and used *in silico* metrics to determine which were most likely to be functional. The sequences were given to Tool Developers for sequence screening by their tools, which had variability in their detection capabilities. Some Tools Developers subsequently modified or updated their tools to identify synthetic homologs and performance improved. The authors did not physically produce the protein variants to test their functionality, however we can assume that design capabilities will continue to improve and that more of the AI-generated sequence variants will successfully perform the function for which they are designed. Efforts such as this are therefore critical for evaluating sequence screening capabilities and developing patches, as needed, for resilience to AI-designed synthetic homologs.

SOC Databases

Sequence screening relies on SOC databases for determining if an ordered sequence is “of concern.” Within these databases, SOCs are generally annotated according to their function, organism of origin, and/or risk level, which can streamline Provider decision-making around follow-up screening and fulfillment. SOC databases could also be used as sequence pools from which to draw sequence test sets for assessing sequence screening capabilities (see below). As approaches to identifying sequences of concern continue to expand beyond lists of regulated agents (see above), key issues arise with regard to the development and maintenance of SOC databases.

Database Security and Access

In the coming years, SOC databases will (continue to) expand beyond sequences unique to regulated taxa. They could contain sequences that have not been uploaded to GenBank due to safety or security concerns. They will encompass sequences that have been identified as contributing to harm from unregulated (in addition to regulated) taxa. As a result, a nefarious actor may be less successful in speculating about which sequences are or are not included. SOC databases could thus pose an information hazard if not adequately secured. However, if overly secured, such databases cannot be used by the stakeholders who need them to screen or to advance screening capabilities.

For example, The Common Mechanism is maintained and hosted by the International Biosecurity and Biosafety Initiative for Science (IBBIS) as an open-source screening tool.[13] Thus, the associated biorisk database is widely accessible. This approach favors ensuring that any and every Provider has the capability to screen and focuses on sequences of known hazards. This minimizes information hazards, as the sequences from regulated agents are all publicly accessible. However, when these databases are expanded to genes from both regulated and unregulated taxa that contribute to harm, additional security precautions may be necessary. By including sequences from unregulated taxa, a SOC database would simplify an actor’s search for hazardous sequences, which might have otherwise required

technical expertise to search through academic publications. It might also enable a bad actor to surmise how likely screening is to flag sequences they intend to use.

SecureDNA, a Tool Developer, takes an alternative approach to database security. Their SOC database was created by breaking SOCs and SOC variants into pieces. The pieces were converted into cryptographic hashes.[14] A Provider using SecureDNA's software (Synthclient) inputs a sequence which is digested using the same hash function. The customer sequence hashes are screened against those in the SOC database. Matching hashes indicate the customer has ordered a SOC. The hashing approach keeps the contents of the database secure and the provided sequence private (from the Tool Developer) without needing to restrict access.

Ultimately, the developer of any SOC database should seek to balance their security practices with the content of their database, distribution, and intended users. Databases that exclusively contain all sequences from regulated agents and organisms do not pose a significant information hazard as lists of regulated agents and their associated sequences are available in public databases. A database of sequences from regulated agents may pose more of an information hazard if it exclusively contains SOCs (not all sequences) from regulated organisms, and particularly so if they have been extensively annotated. Developers of SOC databases that contain new and emerging threats, sequence variants with intensified effects, and/or sequences that are of significant concern should thoroughly consider their database access and security practices.

Development of a Centralized SOC Database

Workshop participants discussed the feasibility and desirability of making a centralized SOC database as opposed to reliance on databases curated by individual Tool Developers or Providers. Some thought that such a database would result in more consistent screening decisions and greater defensibility in screening decision-making, particularly if USG developed or endorsed the centralized database. However, USG lacks the mandate and funding to build and maintain a centralized, accessible database of SOCs. Depending on the database contents and comprehensiveness, USG would face sharing constraints that would limit database utility for Providers and hinder international harmonization of screening practices.

A SOC database developed by the private sector may not receive broad support and adoption. Tool Developers have invested significant time and funds to develop their own proprietary databases, and they are largely working well, alerting Providers not just that a sequence hit to the SOC database, but also communicating information that can help Providers make decisions about whether or not to fill an order. To see significant adoption, a private, centralized database would need to offer some substantial benefit over existing systems. Perhaps such a database could be licensed by Tool Developers in support of standardization across tools. This may be more feasible if Tool Developers are actively involved in the curation of the database, as Tool Developers are unlikely to abandon the SOC databases they have spent years curating and updating.

Regardless of the owner/developer, a centralized database would require *significant* resources to comprehensively reflect all SOCs in the published literature, especially if looking beyond regulated agents. It is not uncommon for developers of SOC databases to find previously published papers that cause them to add a sequence or change its annotation. Even if a database developer was able to accomplish such a feat, the database would quickly become outdated without significant investment in its maintenance. New research is constantly published that may impact whether a given sequence is considered "of concern." For example, a protein of unknown function may be characterized and revealed to have a significant impact on pathogen virulence, clarifying its status as a sequence of concern. Furthermore, the OSTP Framework and HHS Guidance both comment that sequences known to have concerning functions, even when not from regulated agents, should be treated as SOCs "as soon as it is practical to do so" (HHS Guidance) or by October 2026 (OSTP Framework). This paradigm shift will necessitate changes to databases that presently focus only on sequences from regulated agents, potentially requiring their curators to undertake massive searches of published literature to curate and annotate a much broader swath of sequences. Finally, changing public health realities can also impact which sequences are deemed to be of concern.

Variability between SOC Databases

Different screening philosophies, threat models, and perspectives can greatly influence what is or is not included in a SOC database, even when a database developer is trying to only include biosecurity relevant sequences from regulated organisms. For example, amongst existing screening tools, some assume a sequence from a regulated agent is "innocent until proven guilty." Other tools assume these sequences are "guilty until proven innocent," which would greatly expand both the number and types of sequences of concern in a database.[§] If a centralized sequence of concern database were to be used across screening Tool Developers and/or synthetic nucleic acid providers, the database owner(s) would a) need to share the assumptions used in its development with users; b) establish a process by which a rough consensus could be reached on given sequences or types of sequences, such that all stakeholders agreed to use the centralized database; and/or c) compel stakeholders to adopt the centralized database.

In light of the difficulties in the creation and maintenance of a single centralized and secure SOC database, stakeholders agreed that focusing on developing stronger, unified risk-based definitions or criteria for identifying SOCs would more meaningfully improve biosecurity in the near-term. This would enable stakeholders to discuss sequence hazards using the same language and facilitate convergence on a sequence's level of concern. Over time, SOC databases developed by different parties would become more similar, and the challenges of securing a single centralized SOC database could be alleviated.

Advancing Screening Capabilities

Screening capabilities have advanced significantly since the original 2010 HHS Guidance recommended that Providers screen sequences over every 200 basepair segment. Looking forward, both the OSTP Framework and 2023 HHS Guidance recommend narrowing screening specifications.[15] Some participants expressed concern about the potential for a nefarious actor to split up a concerning sequence and order it piecemeal from different Providers. While recognized as a valid concern,[16] this was ultimately deprioritized given the logistical challenge of pooling all orders across companies to look for such splitting in addition to the need to preserve Customer confidentiality.

Test Sets

Conformity Assessment Test Sets

Section 4.4(b)(ii)(D) of AI EO 14110 directed NIST, with industry and other stakeholders, to consider mechanisms for "conformity assessment" of nucleic acid screening systems. A conformity assessment measures performance of a system against a clearly articulated standard, in this case, the definition of a sequence of concern articulated in the OSTP Framework. Sequences used in a conformity assessment should unambiguously be of concern or benign to ensure that conformity assessment results are not subject to debate. Results should not be used to compare Providers, since passing a conformity assessment indicates that a Provider's sequence screening practices are minimally sufficient. From the Provider perspective, a conformity assessment can provide confirmation that implemented practices are sufficient for Framework adherence and self-attestation.

In early 2024, NIST began the development of an attestation test set as a first step towards conformity assessment. This initial test set is intended to help Providers determine if their sequence screening sufficiently adheres to the Framework. An early version given to several screening Tool Developers highlighted challenges in determining which sequences are "of concern" and which are not. The Framework defines a SOC as:

> *a nucleotide sequence or its corresponding amino acid sequence that is a Best Match to a sequence of federally regulated agents (i.e., the Biological Select Agents and Toxins List (BSAT), or the Commerce Control List (CCL)), except when the sequence is also found in an unregulated organism or toxin.*

[§] Notably, a discussion of this question at EBRC's in-person workshop spurred the development of a manuscript currently in preparation.

Tool Developers, hearkening to the HHS Guidance,** did not flag sequences that *are* from regulated agents, but that *do not* pose pathogenic or toxicity risk. This caused their tools to return many negatives that NIST expected to be flagged, based on the Framework SOC definition. After USG interagency discussion and engagement, a second NIST test set was developed, comprised of 1000 x 200 base pair sequences, including 500 true positives (250 viral, 250 bacterial) and 500 true negatives (250 viral, 250 bacterial), taken from public databases. This second version ensured that sequences were unique to regulated pathogens in both nucleotide and protein sequence. In the case of bacteria, sequences were limited to entries from the Virulence Factor Database.[17] In the case of viruses, sequences were limited to those in UniProt annotated with the Gene Ontology (GO) term GO:0019049 (virus-mediated perturbation of host defense response). A subset of these sequences were then blinded and distributed to Tool Developers to run through their systems. All participating Tool Developers conformed to the suggested metrics described below.

NIST developed the current attestation test set as a part of a 2-year pilot project with dedicated resources due to expire in FY25. *The Nucleic Acid Standards for Biosecurity Act*,[18] a bipartisan bill introduced in the summer of 2024 would have authorized $5,000,000 per year through 2029 to NIST to continue its work in the development of screening best practices, implementation, and conformity assessment. The bill did not pass, and it remains to be seen how/if the next Congress and Administration will prioritize securing nucleic acid synthesis. Without funding, NIST is unlikely to continue efforts related to sequence screening, including those related to the development conformity assessment test sets, and another entity trusted by Providers would need to take on this role. USG could encourage such trust through an implicit or explicit endorsement of such an alternative entity.

Administration and Maintenance of an Attestation Test Set

While Tool Developers were useful partners in the initial testing and validation of the attestation test set developed by NIST, stakeholders discussed that evaluation should be conducted at the Provider level. Tool Developers cannot necessarily control how Providers implement their screening tools, and many tools have parameters that can be changed by Providers, influencing which sequences are flagged. Furthermore, Providers, not Tool Developers, are the party responsible for screening in the OSTP Framework and HHS Guidance and thus should be the parties responsible for demonstrating conformity.

As noted above, all Tool Developers performed well with the second version of NIST's attestation test set, meeting proposed accuracy and recall metrics. Accuracy ([true positive calls + true negative calls] / total sequences) captures a screener's false positives and false negatives. Recall (true positive calls / total positive sequences) was deemed the most critical metric as false negatives (failing to identify a SOC) are a greater hazard than false positives (labeling a benign sequence as a SOC). Researchers from NIST leading this first iteration of attestation test set development proposed that Providers have at least a 75% accuracy score and at least 95% recall (5% false negative rate) score, without any expressed dissent from workshop participants.

The OSTP Framework does not require that Providers pass a sequence screening performance baseline test in order to self-attest to adherence, but if or as it becomes a common industry practice, it may become a de facto industry standard and/or integrated into future Framework updates. Thus, Providers should contribute to the development of standards needed in support of more rigorous conformity assessment schemes. This will support higher quality conformity assessment and increase the likelihood of industry-wide adoption. Through recurring testing and evaluation, it is expected that the Providers will generate data to support continuous improvement of sequence screening practices.

EBRC asked stakeholders to identify appropriate entity(s) that could administer and/or maintain the attestation test set. Some suggested a government entity, as it could boost Provider confidence that passing the assessment sufficiently demonstrates OSTP Framework screening adherence. A government agency would need to have the

** HHS Guidance Section V: "In addition, Providers may wish to consider developing solutions for determining which sequences from pathogens should not cause concern (i.e., pass list of genes that pose no pathogenic or toxicity risk)"

authority, staffing, and funding for this purpose, and it does not appear that any agency is currently positioned to take this on.

Alternatively, stakeholders discussed the pros and cons of having a non-governmental organization (NGO) administer evaluation via the attestation test set and subsequent conformity assessments. NGOs could also face political and funding constraints but may have more maneuverability. An NGO might also be more trusted by foreign Providers operating within the US market and beyond. However, an NGO would need to establish its legitimacy with Providers and secure ongoing funding to properly staff and resource conformity assessments in perpetuity. Stakeholders discussed IBBIS, IGSC, and EBRC as potential hosts and administrators of conformity assessments. Most agreed that IBBIS, due to its international focus and technical expertise, would be most appropriate. Concerns about a potential conflict of interest, since IBBIS developed the Common Mechanism screening tool, were raised, but ultimately not considered disqualifying since the Common Mechanism is an open access tool, and conformity assessment would be conducted at the Provider—not Tool Developer—level. As of December 2024, IBBIS is preparing to administer the NIST attestation test set, at least in the short term.

Funds are also required for conformity assessment administration. IBBIS is exploring how it might sustainably fund this service. A fee-for-service model, where Providers pay for conformity assessment, could be feasible, particularly if conformity assessment becomes an industry requirement. Lacking that, Providers might be unwilling to pay for assessment. A relationship between the conformity assessment administrator (i.e., IBBIS) and the host of self-attestations (i.e., JHCHS) could incentivize conformity assessment, particularly if JHCHS were to note that a self-attestation was supported by a passing performance on a conformity assessment. Philanthropy could potentially support IBBIS in this role initially, but a plan for sustainability would be needed.

Benchmarking Test Sets

While attestation test sets are necessary to establish the baseline SOC screening in support of the immediate OSTP self-attestation requirement, additional test sets, such as a benchmarking test set, would be useful to more deeply evaluate Provider screening systems and enable industry-wide improvement of screening practices. A benchmarking test set, in contrast to a conformity test set, would include sequences that may have more ambiguous risk profiles. Results from benchmarking assessments could be anonymized and used to identify trends and variability in screening systems, enabling discussion and opportunities for improvement.

A group of IGSC members has, over the course of 2024, developed a “Bronze Standard” test set of sequences mostly from regulated agents and organisms, building off a prototype developed in 2023.[19] Four screening Tool Developers ran sequences through their tools and outputs were classified as:

1. “Flag” (of concern);
2. “No Flag” (not of concern);
3. “Optional Flag” (not flagged but not cleared); and
4. “Undetermined” (tools conflicted).

The Bronze Standard test set was completed in September 2024, and now the team is working with additional Tool Developers and building processes to I) further validate flag/no flag designations and II) adjudicate sequences in the “optional flag” and “undetermined” categories. This next iteration will lead to a “Silver Standard.” As more tools developers check sequence designations against their own tools, and differences are considered, this test set could potentially be used to support conformity assessment. “Optional flags” or “undetermined” sequences could be used in benchmarking. And, given that this “test set” is fairly comprehensive, “Flag” sequences could be used as a SOC database.

Whether used as a test set, database, or both, industry will clearly benefit from this work. It should reduce duplicative efforts between Tool Developers to determine which sequences are and are not of concern. It should improve defensibility of decision-making around given sequences—if five tools do not flag a given sequence but a sixth does, the developer of the sixth tool may feel more confident in moving that sequence to “no flag” status, decreasing the number of flagged sequences requiring human follow-up and decision-making.

Ideally, this test set could also be a resource to the developers of test sets for conformity assessment. A conformity assessment test set developer could use the Bronze (or Silver, when available) Standard test set as a base from which to pull sequences, ground-truthed by Tool Developers. Or a conformity assessment test set developer could use the Bronze or Silver standard to check their independently developed test sets against this industry-developed standard.

To protect test set integrity and mitigate information hazards, developers and administrators of benchmarking test sets would need to use appropriate security measures and apply access restrictions to their test sets. Stakeholders agreed that an entity(s) outside of government would be most effective in developing, maintaining, and potentially administering benchmarking test sets. Entities outside of government can more easily invite the participation of researchers at the forefront of molecular and engineering biology into the development of test sets. Such researchers are well-positioned to leverage the newest tools and capabilities in the field to consider how a bad actor may seek to cause harm while evading screening detection.

Ultimately, assessment of nucleic acid synthesis screening systems is important for ensuring baseline levels of sequence screening and for enabling the improvement of sequence screening systems. As the government and private sector stakeholders continue to develop and refine these assessment mechanisms, it is possible that, as has happened in other industries, an auditing paradigm may take shape with recognized parties providing accreditation of screening.

Best Practices

- Creators of SOC databases and test sets should take measures to secure potential information hazards and ensure that these resources are continually updated. Providers and Tool Developers should continually evaluate their screening tools and systems.
  - Developers and managers of Sequence of Concern databases should consider database content and intended users in determining appropriate database security measures and access controls. Databases that contain unencrypted sequences from new and emerging threats, certain sequence variants, and/or SOCs from unregulated agents should implement enhanced security practices.
  - Developers and managers of Sequence of Concern database(s) should have documented and funded plans for improving and maintaining such databases by filling existing gaps and incorporating new research as the biothreat landscape changes.
  - Tool Developers and Providers should, potentially with the assistance of third parties, periodically assess the performance of their tools and sequence screening systems against AI-generated sequence variants that are likely to have conserved function but lack high sequence homology. As possible, patches to AI vulnerabilities should be developed and applied by Tool Developers and/or Providers.
  - When available, Providers should participate in conformity assessments to ensure their screening practices meet relevant standards, such as that set by the OSTP Framework.

Recommendations

- NIST and HHS, along with other relevant stakeholders across USG, should continue to engage with Providers and Tool Developers to develop a more robust conceptualization of “Sequence of Concern,” to develop and improve screening assessment mechanisms, and to identify new threats that may be mitigated by nucleic acid synthesis screening.
  - To prioritize sequence screening resources on sequences that pose the greatest concern, the US Government should fund and/or encourage an enduring and dedicated public-private effort to develop a process for determining whether or not a sequence is “of concern” and its level of risk (6–24 months).
    - In this process, stakeholders should endeavor to define “functions of concern” and, ultimately, the genomic and environmental contexts in which a harmful activity occurs to move toward a “properties of concern” paradigm.
    - Efforts should include, but move beyond, sequences from lists of specific taxa.

        - Parallel efforts may be useful in these early stages while further discussion is needed to improve upon existing "sequence of concern" definitions.
    - Congress should direct NIST to continue its engagement with industry to support the development of conformity assessment schemes and standards for nucleic acid synthesis screening (3-48 months).
        - NIST is uniquely positioned to develop standards and conformity assessment schemes in support of evolving biothreats.
        - While important progress has been made by NIST in 2024 toward the establishment of standards, best practices, and mechanisms for the assessment of screening practices, the advancement of AI-supported biodesign, DNA assembly, and sequence screening will require continued work and engagement.
    - USG should continue to support the development of guidance and standards for nucleic acid synthesis screening (on-going).
        - An interagency group including representatives from HHS/ASPR, NIST, NSF, NIH, and DHS should continue to meet regularly. This group could provide guidance to industry based on industry needs and, further, support non-governmental efforts to develop robust "Sequence of Concern" definitions or matrices, screening testing and evaluation methodologies, and best practices domestically and internationally.
- Providers should identify and engage with third-parties, like IBBIS and USG entities, to enable independent verification of screening best practices and monitor emerging dual-use technologies like AI/ML-enabled Biodesign Tools.
    - A third party, trusted by public and private stakeholders, should administer conformity assessments for the nucleic acid synthesis industry (3-12 months).
        - Conformity assessment scoring should take frequency of false positives and false negatives into account and use sequences that are as unambiguous as possible.
        - Ideally, the entity administering NIST's attestation test set should be trusted by Providers internationally and domestically.
        - A strong foundation of voluntary conformity assessment would enable industry-led accreditation practices in the future.
    - Private-sector organization(s) should develop benchmarking evaluations of nucleic acid synthesis screening systems to identify points of divergence between Providers and enable conversation and analysis that supports improved screening industry-wide (6–12 months).
    - The NIST AI Safety Institute should work with industry to support regular assessment of the resilience of screening tools to synthetic homolog sequences designed by state-of-the-art Biodesign Tools (indefinite).
        - Recent work suggests that the security challenges associated with advanced Biodesign Tools can be mitigated, but such mitigation efforts must keep pace with advances in Biodesign Tools. Coalitions within the private sector, and/or public-private partnerships, may be best for bringing the needed stakeholders and expertise to the table to enable this work.
    - Providers and/or Tool Developers should regularly test the resilience of their screening systems and tools to AI-designed sequences of concern (indefinite).
        - While tools currently perform well against AI-designed sequences, sequences designed with de novo design capabilities may be less detectable by tools that rely on homology. Regular testing can help Tool Developers understand any emerging vulnerabilities in their systems.
        - Improved functional prediction given a sequence is on the near horizon. As these capabilities develop, Providers and/or Tool Developers should consider incorporating them into screening.

References

1. Godbold GD, Hewitt FC, Kappell AD, et al. Improved understanding of biorisk for research involving microbial modification using annotated sequences of concern. *Front Bioeng Biotechnol.* 2023;11. doi:10.3389/fbioe.2023.1124100
2. Gemler BT, Mukherjee C, Howland CA, et al. Function-based classification of hazardous biological sequences: Demonstration of a new paradigm for biohazard assessments. *Front Bioeng Biotechnol.* 2022;10. doi:10.3389/fbioe.2022.979497
3. Godbold GD, Kappell AD, LeSassier DS, Treangen TJ, Ternus KL. Categorizing Sequences of Concern by Function To Better Assess Mechanisms of Microbial Pathogenesis. *Infection and Immunity.* 2022;90(5):e00334-21. doi:10.1128/iai.00334-21
4. National Academies of Sciences, Engineering, and Medicine. Biodefense in the Age of Synthetic Biology. *The National Academies Press*. 2018. doi: https://doi.org/10.17226/24890.
5. The Gene Ontology Consortium, Ashburner M, Ball CA, et al. Gene Ontology: tool for the unification of biology. *Nat Genet.* 2000;25(1):25-29. doi:10.1038/75556
6. jhuapl-bio/pathogenesis-gene-ontology. GitHub. Accessed January 24, 2025. https://github.com/jhuapl-bio/pathogenesis-gene-ontology/blob/master/pathgo.obo
7. Resnick P. On Consensus and Humming in the IETF. Internet Engineering Task Force; 2014. doi:10.17487/RFC7282
8. Abramson J, Adler J, Dunger J, et al. Accurate structure prediction of biomolecular interactions with AlphaFold 3. *Nature.* 2024;630(8016):493-500. doi:10.1038/s41586-024-07487-w
9. Krishna R, Wang J, Ahern W, et al. Generalized biomolecular modeling and design with RoseTTAFold All-Atom. *Science.* 2024;384(6693):eadl2528. doi:10.1126/science.adl2528
10. Boadu F, Lee A, Cheng J. Deep learning methods for protein function prediction. *PROTEOMICS.* 2025;25(1-2):2300471. doi:10.1002/pmic.202300471
11. Dauparas J, Lee GR, Pecoraro R, et al. Atomic context-conditioned protein sequence design using LigandMPNN. *bioRxiv.* Preprint published online December 23, 2023:2023.12.22.573103. doi:10.1101/2023.12.22.573103
12. Wittmann BJ, Alexanian T, Bartling C, et al. Toward AI-Resilient Screening of Nucleic Acid Synthesis Orders: Process, Results, and Recommendations. *bioRxiv.* Preprint published online December 4, 2024:2024.12.02.626439. doi:10.1101/2024.12.02.626439
13. Wheeler NE, Carter SR, Alexanian T, Isaac C, Yassif J, Millet P. Developing a Common Global Baseline for Nucleic Acid Synthesis Screening. *Applied Biosafety.* 2024;29(2):71-78. doi:10.1089/apb.2023.0034
14. Baum C, Berlips J, Chen W, et al. A system capable of verifiably and privately screening global DNA synthesis. *arXiv.* 2024. doi:10.48550/arXiv.2403.14023
15. Kane A, Parker MT. Screening State of Play: The Biosecurity Practices of Synthetic DNA Providers. *Applied Biosafety.* 2024;29(2):85-95. doi:10.1089/apb.2023.0027
16. Crawford FW, Webster K, Epstein GL, Roberts D, Fair J, Nevo S. Securing Commercial Nucleic Acid Synthesis. *RAND Corporation.* 2024. www.rand.org/t/RRA3329-1
17. VFDB: Virulence Factors of Bacterial Pathogens. Accessed January 24, 2025. https://www.mgc.ac.cn/VFs/main.htm
18. Rep. Caraveo Y [D C 8. Actions - H.R.9194 - 118th Congress (2023-2024): Nucleic Acid Standards for Biosecurity Act. September 11, 2024. Accessed January 24, 2025. https://www.congress.gov/bill/118th-congress/house-bill/9194/all-actions
19. Wheeler NE, Bartling C, Carter SR, et al. Progress and Prospects for a Nucleic Acid Screening Test Set. *Applied Biosafety.* 2024;29(3):133-141. doi:10.1089/apb.2023.0033

Customer Screening

Customers of nucleic acid synthesis Providers include academic research scientists—such as faculty, staff, students, and other trainees—at colleges and universities, independent researchers at non-profit organizations, scientists at companies or private research institutions, and biology hobbyists at "Do It Yourself" (DIY) community laboratories. A small proportion of these Customers, working with their biosafety officers and following applicable guidance and/or regulation, conduct legitimate and peaceful research on hazardous viruses and organisms of concern, working to understand their biology and support the development of life saving diagnostics, therapeutics, and vaccines. Such Customers are aware of and trained on the precautions, safety, and controls of these materials. They often have years or decades of experience utilizing these genetic sequences, and depending on the nature of their work, may utilize high-containment facilities. Customer screening enables Providers to ensure that such Customers can access the sequences they need for this important work, while preventing unqualified Customers or Customers without a legitimate need from obtaining them.

Providers should work to confirm Customer identity for all orders, and to confirm Customer legitimacy for orders containing a SOC (Fig. 3). Elements of identity verification can occur after account creation and/or after an order is placed and may include confirming that the Customer organization is associated with life sciences research, that the payment information matches the Customer information, checking the Customer name against Restricted Party Screening systems, and/or other measures. The verification of legitimacy for Customers ordering a SOC is a more significant challenge. During EBRC's workshops, stakeholders considered methods for establishing Customer identity and legitimacy, what information from Customers would be most definitive for establishing identity and legitimacy, and profiles of Customers that may have ambiguous legitimacy and how to handle them.

Central Issues and Perspectives

Customer Identity Verification

The OSTP Framework directs Providers to "assess" Customer identity for all orders, while the HHS Guidance recommends that Providers "verify" Customer identity for all orders. A clear standard for Customer identity verification does not exist for nucleic acid screening, which may account for the difference in language. Moving forward, it would be helpful to develop standardized identity verification practices, recognizing that, if such practices are to be implemented for each order, they cannot require (significant) human action. Some basic identity verification strategies might include screening email addresses for domains matching their listed institution, and/or for ".org," ".edu," or other appropriate domain extensions. Providers could verify email addresses through an email link verification and could confirm that the given shipping address matches the Customer's stated institutional affiliation. More stringent identity verification, in addition to verification of legitimacy, may be appropriate when an order contains a SOC.

NIST's Draft Standard Guide (Annex III) for supporting attestation under the OSTP FW lists information that Providers should request during the identity verification (and legitimacy verification, see below) process. Minimally, Providers should collect the following information:

- Customer name
- Customer institution or affiliation
- Address
- Phone number
- Email

Providers should also ask the Customer if their order contains a SOC, and if so, ask the Customer to provide information to demonstrate legitimacy (see below). In parallel with EBRC workshops, the International Biosecurity and Biosafety Initiative for Science (IBBIS) has been developing Customer screening forms that could be used across

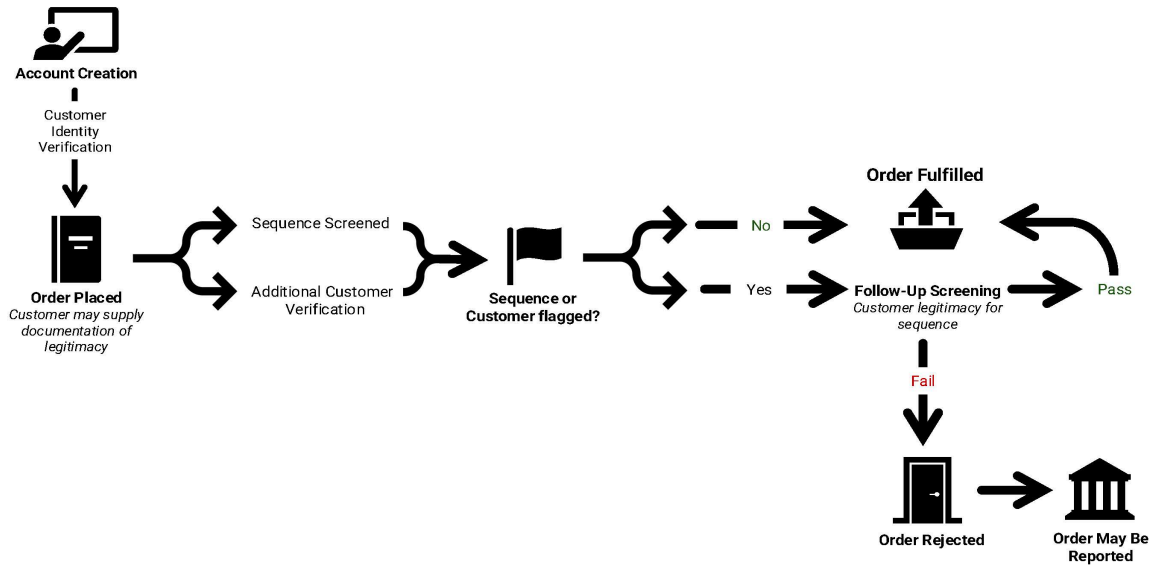

Figure 3: Generalized nucleic acid synthesis screening workflow. Customers create an account with a given Provider to order nucleic acids. Providers should verify Customer identity for every order; some elements of identity verification may take place before an actual order is placed (e.g., verification of institutional email address), while other elements of identity verification may occur after an order is placed (e.g., payment method verification). Ordered sequences are screened to identify possible Sequences of Concern (SOCs). If an order is flagged for any reason, follow-up screening to confirm order legitimacy is initiated. Follow-up screening can use information provided by the Customer at the account creation stage, at the order placement stage, or through direct Customer contact, and/or may use publicly available information. Orders that pass this screening, or which did not have a flag to begin with, are fulfilled. Flagged orders that fail follow-up screening are rejected. Rejected orders may be reported to law enforcement.

life sciences providers, in addition to decision support guidance. Ideally, different efforts will converge upon the same set of information to collect, and congruous methods for identity verification.

Oftentimes, in research laboratories, a Principle Investigator or senior researcher creates an account for ordering nucleic acids and shares the login credentials with lab members. Thus, even if the account owner's identity is verified, a Provider may not be able to verify the user identity for each order. This presents a potential security risk. Should Providers be responsible for verifying the identity of each potential end user of such an account, or is verification of the account holder during account creation sufficient? Stakeholders considered several methods for potential identity verification of individual account users, including:

1. Requiring each individual user to have a personal account. Account users could be verified through multi-factor authentication (MFA) at the time of ordering, which could prevent password sharing. However, this level of granularity and account security would likely not be feasible and difficult to implement given that:
    a. academic labs have transient researchers such as undergraduates and rotating graduate students. To avoid setting up new accounts for each person, lab members would likely share credentials and blindly provide MFA for one another; and
    b. sharing one account per research group has some advantages. It centralizes a group's ordering, giving principal investigators or other responsible parties oversight of lab orders.
2. Having a single account for a research group that would require PI sign off or PI MFA before being produced by a Provider. However, routing all orders through one individual could slow and impede normal laboratory operations were that individual, e.g., to fall ill or travel.

3. Setting up an administrative account for principal investigators or other responsible parties through which individual accounts for lab members, each verified through MFA, could be set up. The owner of the administrative account could then be notified any time a SOC was ordered by one of their authorized accounts, and individual accounts could be easily created or deleted as group members joined and left.

Ultimately, participants emphasized that it would be extremely difficult to stop research groups from sharing credentials. Rather, it is more appropriate for Providers to verify the identity of the main account holder, who then takes responsibility for being able to identify which group member ordered a given sequence.

Verifying Customer Legitimacy

The verification of Customer legitimacy confirms that a Customer has a real, peaceful, life sciences-oriented use for a given SOC, and that the Customer's institution "has a life sciences-oriented mission and purpose, or uses synthetic nucleic acids for other relevant applications."[1] Traditionally, follow-up screening to verify legitimacy has been done after a SOC is flagged. Customers should now be encouraged to provide such information up front (see Draft Standard Guide, Annex III), which can decrease the time and resources Providers must dedicate to follow-up screening and the time it takes to ship an order. Still, Providers and Customers face uncertainty as to what types of documentation are sufficient to demonstrate legitimacy, whether provided during the ordering process or as a result of follow-up screening by a Provider.

The HHS Guidance, the HHS Guidance Companion Guide, and the OSTP Framework each give consistent information for establishing Customer legitimacy, as does a review article[2] whose authors worked on the development of the HHS Guidance. Legitimacy can be established with information such as the proposed use for the order, the contact information for a biosafety officer (or equivalent representative), any documentation of institutional review of the research, proof of registration with the Federal Select Agent Program (FSAP), publication history, grant numbers, etc.[††] Providers can confirm that the shipping address has appropriate laboratory facilities, as well as cross-referencing whether laboratory websites list the Customer name and relevant research.

Table 2 provides a useful guide for the types of information that can demonstrate legitimacy. This table also highlights that different types of information carry different weight in determining Customer legitimacy. While some information on its own could be considered sufficient for verifying legitimacy (e.g., evidence of FSAP registration), other types of information may require additional corroborating details (e.g., research plan, grant number(s)).

In the future, it could be useful to attempt to break down the types of information needed for sequences with different risk profiles. Parameters for verifying legitimacy might be more stringent when a sequence from a viral tier 1 Select Agent is ordered than, for example, a gene of unknown function from a fungal pathogen. This approach could potentially be integrated into screening tools, many of which already stratify SOCs into tiers. Given tiers could have associated information types necessary to establish legitimacy.

Regardless of tiering, standardization of information required when purchasing SOCs could help to normalize expectations of Customers. Without consistent and standardized questioning and information requirements between Providers, Customers may become frustrated with or resistant to providing information to demonstrate legitimacy, either out of concern for their intellectual property or because providing the needed information is considered too burdensome. Having a Standard Guide such as that developed by NIST/EBRC/IGSC widely adopted by industry could help to normalize and socialize such information collection.

Another workshop topic of discussion focused on whether greater emphasis should be placed on confirming individual or institutional legitimacy. Business documents may not be particularly useful to startup Providers who may lack the resources to verify the veracity of such documents, especially for organizations outside of their country (e.g., incorporation documents in another language). Alternatively, a researcher may have a large gap in visible

[††] Pg 11, footnote 14; https://www.whitehouse.gov/wp-content/uploads/2024/04/Nucleic-Acid_Synthesis_Screening_Framework.pdf

Type of information	*Useful by itself*	*Useful in combination*
Documentation of internal review and approval of the project/research, such as by an IBC	✓	
Registration with FSAP	✓	
Statement by Ultimate Consignee and Purchaser (i.e., a completed BIS-711 form)	✓	
Business license(s)		✓
Grant number(s)		✓
Institutional or corporate affiliation		✓
Name of the institutional biosafety officer		✓
Open researcher and contributor identifier		✓
Other legitimate use (e.g., diagnostic test development or manufacture)		✓
Proposed end use of the order		✓
Publication history		✓
Research plan		✓

Table 2 (Adapted from Sharkey, et. al. 2024[2]): Examples of customer information that could be supplied to Providers to establish legitimacy.

research and publication (i.e., perhaps they worked on proprietary research in industry), but if working for a reputable institution, may still be deemed legitimate.

Despite useful Federal guidance on the demonstration of Customer legitimacy, the reality of unique Customer situations necessitates that Providers use their independent best judgement and conduct adequate follow-up, where deemed necessary. In doing so, Providers will always face the tension of appropriate screening and preservation of resources. These Providers have a negative financial incentive to conduct robust Customer investigation, because expanding their Customer screening procedures means smaller margins on each order and potentially worsening Customer experience. Because of these challenges, it is worth considering how/if verifying Customer legitimacy can be streamlined or standardized, or if the responsibility and expense of verifying Customer legitimacy can be distributed beyond Providers.

alleviating the burden of legitimacy verification is to incorporate Customer screening into sequence screening tools, such as that which is currently offered by Aclid, Inc. Another option is to involve biosafety or other relevant professionals from the Customer's institution in the ordering process. Such individuals should have direct knowledge of projects within their institutions with a legitimate need for SOCs. However, institutions have different types of biosafety and biosecurity staff and infrastructure. They may not have bandwidth to take on such a significant role, and may not always have the expertise for judging specific sequences.

Another option is to develop a pre-authorization process for Customers that have a legitimate need to regularly order SOCs. A third-party would verify that a given Customer is undertaking legitimate research and may require access to certain types of SOCs. The third-party would issue a certificate to the Customer, that, when given to a Provider, would obviate the need for the Provider to verify legitimacy. This would ease the burden on Customers whose research involves agents containing SOCs and ease the follow-up burden on Providers. This line of conversation during an EBRC workshop prompted a group of stakeholders, led by SecureDNA, to independently explore such a potential credentialing mechanism. This approach is not without challenges. For example, an authorizing third party would need to establish trust with Providers. Some stakeholders argued that creating a privileged "pass list" of Customers would make those Customers a prime target for phishing attacks. A list of privileged Customers also presents issues with equity and bias that could favor research groups with more financial resources. Because of these challenges, some advocated for a "zero trust" model instead.

Best Practices

- Providers should strive to verify Customer identity for every order, and in the case of SOC orders, strive to implement screening practices and information collection that ensures Customers seeking SOCs have a legitimate, safe, and peaceful purpose for those SOCs.
  - Providers should collect standardized identifying information from each Customer during the ordering process including, minimally, name, affiliation, address, phone number, and email, and should ask Customers if their order contains a SOC when submitting orders.
    - If a Customer indicates that their order does or might contain a SOC during the ordering process, follow up prompts should ask for the information of the End User (if different than Customer), intended use, applicable biosafety and biosecurity oversight, contact information for biosafety and/or biosecurity official(s), and Biosafety Level (BSL) of the Customer's laboratory.
  - Providers should implement reasonable mechanisms to verify the identity of Customers (regardless of whether or not they are ordering SOCs). Such verification could include automated email verification or a mechanism to confirm that shipping addresses match given institutions.
    - These processes should be automated to minimize Provider burden.
    - Providers cannot be responsible for verifying the identity of all users when account credentials are shared within a research group.
  - When a Customer orders a SOC, Providers should verify Customer and Institutional legitimacy before fulfilling the order.
    - Customer legitimacy may be demonstrated by describing the proposed use for the order and by providing the contact information for a biosafety officer, documentation of institutional review of the research, proof of registration with the FSAP, publication history, grant numbers, etc. See Table 2 for documentation that can demonstrate legitimacy.
    - Orders for SOCs should not be fulfilled without the receipt of contact information for an individual at the institution who is responsible for biosafety and/or biosecurity.
  - When Customer legitimacy cannot be verified for orders containing SOCs, Providers should decline to fulfill the order.

Recommendations

- USG should fund an entity, such as NIST, to continue engaging with Providers, biosecurity experts, and other relevant stakeholders to synthesize robust methods for performing risk assessments on SOC orders.
  - A government entity such as NIST should engage Providers, academics, and biosecurity experts to matrix SOC tiers against needed evidence for the demonstration of Customer legitimacy (12–36 months).
    - Not all SOCs warrant the same degree of concern. Providers should be encouraged to gather only as much information as necessary to verify that a given Customer is a legitimate user of a given sequence.
    - Creating such a matrix first requires describing tiers of potential concern for sequences and customers. This would take significant time if approached at a community level, but may be significantly easier to build within existing screening tools that already divide SOCs into tiers.
  - NIST should continue to engage with Providers and other stakeholders to develop and encourage the adoption of standards for verifying Customer identity and Customer legitimacy (6–12 months).
    - If information gathering was standardized across Providers, Customers would come to expect to be asked for certain types of information when ordering nucleic acids. Such a standard would give Providers defensibility in the face of Customer pushback.
    - Such standards would communicate to Providers the level of due diligence that is appropriate for follow-up screening.
- Providers should pursue new methods for establishing Customer identity and legitimacy, including engaging third parties on new security technologies.
  - Providers should implement systems to confirm Customer identity through multiple factors like email or phone number verification at the time of account creation (6–12 months).
  - USG or another funder should fund an analysis of third-party Customer legitimacy verification options (6–18 months).

References

1. United States National Science and Technology Council, Fast Track Action Committee on Synthetic Nucleic Acid Procurement Screening. *Framework for Nucleic Acid Synthesis Screening*. U.S. NSTC. 2024. https://aspr.hhs.gov/S3/Documents/OSTP-Nucleic-Acid-Synthesis-Screening-Framework-508.pdf
2. Sharkey CM, Lekveishvili M, De La Rosa T, Danskin K. Enhancing Gene Synthesis Security: An Updated Framework for Synthetic Nucleic Acid Screening and the Responsible Use of Synthetic Biological Materials. *Applied Biosafety.* 2024;29(2):63-70. doi:10.1089/apb.2023.0036

Law Enforcement Reporting

Providers are encouraged by the HHS Guidance and OSTP Framework to report suspicious purchase orders to law enforcement agencies, specifically to local FBI Weapons of Mass Destruction (WMD) Coordinators, who are placed in FBI field offices around the country. FBI WMD Coordinators act as resources to Providers, and reporting does not necessarily result in action by the FBI. FBI WMD Coordinators are poised to help Providers assess a situation. Still, Providers understandably may feel some hesitance in such reporting. Were a Provider to have a reputation for reporting to the FBI, even legitimate Customers may avoid using that Provider. Anecdotally, uncertainty about when to report, and the consequences or impacts of doing so, have resulted in widely varied reporting practices between Providers. EBRC engaged with stakeholders on some of the uncertainties surrounding law enforcement reporting.

Central Issues and Perspectives

Decision Making Around Law Enforcement Reporting

Providers have different approaches or thresholds for reporting suspicious orders. The permutations of Customers and sequences are enormous, making it challenging to set well-defined reporting thresholds. One approach is to encourage Providers to report any suspicious order for sequences of concern that they do not fulfill after conducting follow-up screening.[‡‡]There may be rational reasons for reporting orders that actually were fulfilled. On the other hand, an order from a naive student for a SOC may not be deemed report-worthy after Provider follow-up.

One ambiguous scenario Providers face is Customer "ghosting," where a Customer stops replying to Provider follow-up screening efforts. Stakeholders were split on whether this situation would necessitate reporting to law enforcement. Some felt that this represented a "red flag," and suggested that such a Customer could be attempting to avoid further scrutiny from a Provider. Reporting such a Customer would allow law enforcement to determine if this Customer was attempting to identify a Provider that will fulfill their order without appropriate screening. Others felt that this situation may be too ambiguous to report in the absence of other red flags. Customers may miss the follow-up email from a Provider or simply not care about the sequence enough to respond, particularly if the flagged sequence is part of a large pool. Reporting such Customers could result in undue scrutiny and divert law enforcement resources away from more pressing needs.

Stakeholders also discussed a potential role for law enforcement in split order detection, where a Customer orders pieces of a SOC from various Providers with the intent to assemble them. Detecting such schemes would require compiling orders across Providers, necessitating coordination or cooperation among them or with a third party. The IGSC has a *very* rarely used mechanism for Provider information-sharing. Providers are reluctant to share Customer information with one another, thus a non-Provider third-party would likely need to lead such an effort. Law enforcement could be a desirable third party in a very limited capacity. It does not have models built to computationally look for split orders, but is well-poised to identify trends in reported orders across Providers.

Ultimately, guide(s) are needed to support Provider decision-making around FBI reporting. Such a guide might also include an intermediate option for Providers short of making a full report. A Provider may gain confidence and/or clarity in decision making in reaching out to an FBI WMD-Coordinator to discuss an order without disclosing the Customer name or details. At present, reporting is based on Provider intuition, which, anecdotally, has resulted in very different reporting practices between Providers.

[‡‡] This approach most closely aligns with the HHS Guidance, which states that "If follow-up screening does not resolve concerns about the order, or if there is reason to believe a customer may intentionally or inadvertently violate U.S. laws or regulations, Providers should not fulfill the order and should contact designated entities within the U.S. government (i.e., U.S. Department of Commerce, Federal Bureau of Investigation [FBI]) for further information and assistance" (pg 2-3).

Best Practices

- Providers should work with their local FBI WMD Coordinator to relay concerning orders and perform risk assessment.
  - Providers should identify their local FBI WMD Coordinator and establish a working relationship.
  - When a Provider is uncertain about reporting an order, the Provider should consider reaching out to local FBI WMD Coordinators to assist in decision making, even if they choose not to disclose the Customer name.
  - Providers should report highly suspicious orders for SOCs to local FBI WMD Coordinators or other relevant law enforcement officials.

Recommendations

- NIST should work with industry to further develop and/or support the development of Customer screening guides that include decision-making support for FBI reporting (12 months).

Record Retention

The HHS Guidance and the OSTP Framework recommend that Providers retain records for at least three years. The HHS Guidance notes that retaining them longer, for up to eight years, is desirable if it does not place undue burden on the Provider. These retained records would be crucial to law enforcement in the event of an investigation following a biological incident, or in attempts to attribute a bio-related crime. Retained records could also be beneficial to the detection of SOCs split across providers. Furthermore, they could be useful to efforts to improve screening or look at screening consistency across Providers, particularly if records include information on how screening was performed and justifications for screening outcomes. For example, it could be useful for a trusted third-party to assess differences in reporting to law enforcement between Providers or types of Providers. Finally, record retention can provide proof of due diligence by Providers and demonstration of their commitment to security and safety. EBRC engaged stakeholders on the types of data and data formats that would facilitate these potential records uses.

Central Issues and Perspectives

Standardizing Provider Record Keeping Practices

As the field aligns on standardized or semi-standardized questions to ask of Customers during the ordering and follow-up processes, record retention should also become more standardized. The Draft Standard Guide (Annex III) encourages Providers to retain records of all information gathered through use of that guide. Stakeholders were in alignment with HHS Guidance that records should be retained for Customer information (purchaser and end user name, email, phone number, organization, and payment type/account) and order information (nucleotide sequence ordered, screening method, screening tool version, screening results, date ordered/shipped, shipping address) for each order, regardless of SOC flags. All records could also include whether or not the Customer self-declared a SOC, if a SOC was flagged during screening, the method of identity verification, the date and time an order was received, and when the order was shipped or declined. Providers could also record Customers' stated descriptions and uses for SOCs, any follow up correspondence between the Provider and the Customer that informed Provider fulfillment, supporting documents provided by the Customer, Provider fulfillment decision and rationale, and information on any law enforcement reporting. Individual Providers likely have their own formatting preferences and file types for these order records. To support records analysis, particularly when criminal intent or activity is suspected, files should be exportable to a common file format with a common structured format.

Beyond their utility to law enforcement, stakeholders also discussed how a unified record format could support a centralized repository of concerning orders. Such a centralized repository could enable the detection of SOCs split across multiple Providers and serve to alert the Provider community to suspicious actors. A third-party, like MITRE (which provides a similar service for aviation safety), a national laboratory, or an NGO like IBBIS, would be desirable for this role, as Providers may be more comfortable disclosing order details to an intermediary that does not have any competing business interests and does not carry the same weight as providing such information to law enforcement. However, even if a third-party were identified that could operate and maintain such a repository, stakeholders expressed doubt that Providers would be willing to share information that could compromise their customers' confidential or proprietary information.

Best Practices

- Providers should record and retain Customer information and order information for at least three years.

Recommendations

- NIST should continue to engage stakeholders on its Standard Guide, and as it is finalized, determine in partnership with industry which information fields should be retained (6–12 months).

Cybersecurity and Information Security

Anecdotally, Providers have been unsure of how best to adhere to OSTP Framework Practice 6: "Take steps to ensure cybersecurity and information security." Larger Providers may already have implemented ISO 27001 (or equivalent third-party certification), but smaller Providers may not have the resources to pursue and obtain third-party certification. The NIST Cybersecurity Framework 2.0 (CSF) and Cybersecurity Supply Chain Risk Management (C-SCRM) documents (e.g., SP 800-161r1),[1] while useful, are detailed and robust in order to encompass many industries. Specific and actionable guidance for the synthetic nucleic acid industry would be useful to Providers. Fundamentally, stakeholders agreed that Providers should take steps to protect Customer identities, personal private information, and intellectual property. They also agreed that SOC databases can pose an information hazard, and thus should be secured proportionally to their content. Individuals from NIST walked stakeholders through these guides, explaining how they might be useful to this industry.

Central Issues and Perspectives

NIST Cybersecurity Framework 2.0 and Cybersecurity Supply Chain Risk Management

NIST led discussions during workshops of its Cybersecurity Framework 2.0 (CSF) and published guidance.[2,3,4] The CSF Core is designed to define high-level cybersecurity outcomes that are broadly applicable to all organizations so that they can understand, assess, prioritize, and communicate their cybersecurity efforts.[2] The CSF describes six key functions (Govern, Identify, Protect, Detect, Respond, Recover) for preventing and responding to cybersecurity incidents. The information contained within the CSF is vast and may seem daunting to Providers. Helpfully, NIST has a CSF 2.0 Quick Start Guide to support potential users from small businesses with no cybersecurity plans in place to large organizations or even communities of organizations.[5] The National Cybersecurity Center of Excellence (NCCoE), also part of NIST, has engaged with industry and government stakeholders to develop Community Profiles for specific industries, such as genomics[3] and artificial intelligence,[6] that can support CSF implementation across similar organizations.

NIST representatives guided in-person workshop participants through a thought exercise to demonstrate the applicability of the CSF to Providers. A Provider Mission Objective of "ensuring SOC orders are only fulfilled to Customers whose identity and legitimacy is established," would be threatened by the loss or inoperability of sequence and/or customer screening capabilities. Thus, a cybersecurity best practice would be to establish capabilities for different operating states, including if primary sequence screening systems were compromised. NIST's Cybersecurity Supply Chain Risk Management (C-SCRM) guide, which is concerned with "identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels," would recognize screening systems as part of a Provider's cybersecurity supply chain. Best practices that are or could be in place include contractual requirements for suppliers of screening tools to provide evidence of security practices to ensure this element of a Provider's cybersecurity supply chain will remain intact.

Best Practices

- Developers of SOC databases should ensure that SOC databases have cybersecurity risk management strategies proportional to their content. Databases containing easily accessible, publicly available sequences from regulated agents and organisms may require less security than expanded databases and/or databases that describe the functions of sequences that may not be widely known to be concerning.

Recommendations

- NIST should engage Providers and government stakeholders on the development of a CSF 2.0 Community Profile for Providers (1–2 years).

— Community Profiles “help an organization put the CSF into practice and set priorities for managing cybersecurity risks.”[2] As many organizations across an industry may face similar cybersecurity risks, Community Profiles help to define and address shared risks to support the industry as a whole.

References

1. Boyens J, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. *National Institute of Standards and Technology (NIST)*. 2024. doi:10.6028/NIST.SP.800-161r1-upd1
2. National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework (CSF) 2.0. *NIST*. 2024; NIST CSWP 29. doi:10.6028/NIST.CSWP.29
3. Pulivarti R, Martin N, Byers FR, et al. Cybersecurity of Genomic Data. *National Institute of Standards and Technology (NIST)*. 2023; NIST IR 8432. doi:10.6028/NIST.IR.8432
4. National Institute of Standards and Technology (US). NIST Cybersecurity Framework 2.0: Resource & Overview Guide. *National Institute of Standards and Technology (NIST)*. 2024; NIST SP 1299. doi:10.6028/NIST.SP.1299
5. CSF 2.0 Quick Start Guides. *National Institute of Standards and Technology (NIST).* Published online December 8, 2023. Accessed January 24, 2025. https://www.nist.gov/cyberframework/quick-start-guides
6. Cyber AI Profile | NCCoE. *National Cybersecurity Center of Excellence.* Accessed January 24, 2025. https://www.nccoe.nist.gov/projects/cyber-ai-profile

Education and Implementation Support

The life sciences research ecosystem is vast, with many types of Providers and Customers or Users. Outside of networks that are particularly attuned to nucleic acid synthesis screening, many stakeholders with responsibilities under the HHS Guidance and/or OSTP Framework may be completely unaware. Stakeholders at EBRC/NIST workshops discussed which stakeholder groups may need additional outreach and education and how they might be reached.

Central Issues and Perspectives

Informational Outreach

Life sciences academic researchers may be completely unaware of the HHS Guidance, OSTP Framework, and/or funder requirements for synthetic nucleic acid procurement.[1] Institutions have a real interest in securing the federal funds of their researchers, thus procurement offices would likely benefit from some awareness of the updated funding award requirements to help ensure compliance. Similarly, Offices of Sponsored Projects within universities should be made aware of these requirements so that requirements can be properly communicated to principal investigators. Outreach across stakeholders at an institution can enable built-in redundancy, supporting research community compliance.

Stakeholders also pointed out that university core facilities that provide DNA synthesis services also may not be aware of the OSTP Framework, HHS Guidance, and/or the actions they should take to continue supporting Customers with federal funding. Under the HHS Guidance and OSTP Framework, core facilities with synthesis capabilities are considered Providers, and if not already screening, should implement systems to do so. Outreach to university administration and directly to core facilities would ensure that these groups are made aware of their responsibilities for screening.

Socialization Strategies

EBRC also led discussions on the most effective channels of communication to reach the relevant stakeholders. Some experts recommended coordinating with professional associations like the National Association of College and University Business Officers and the Council on Governmental Relations to reach university administration and procurement offices. To reach Providers, stakeholders recommended trade shows and conferences like SynBioBeta and Bio-Innovation Week. Organizations with Provider membership, like the IGSC and Bioeconomy Information Sharing and Analysis Center (Bio-ISAC), also play an important role in socializing screening best practices and norms. Trade journals focused on biotechnology or government contracts may be a good way to reach a variety of stakeholders in print.

Regardless of how stakeholders first learn about relevant U.S. policy, a central resource repository would be incredibly useful for finding additional information and context. In addition to hosting self-attestation forms, JHCHS has developed a website[2] that contains background information and documents, answers to frequently asked questions, and links to resources that explain relevant policy for Providers, manufacturers of benchtop nucleic acid synthesizers, and Customers. Hosting attestations along with this informational material would be beneficial, as traffic to the site will be driven by Customers seeking out lists of self-attesting Providers, boosting the informational material that is included alongside it.

Best Practices

- Providers, along with research institutions, should ensure that the OSTP Framework, HHS Guidance, and updated NIH funding requirements are properly socialized to Customers and awardees.
  - Providers and other members of industry should socialize U.S. nucleic acid synthesis screening policies with their Customers to spread awareness and encourage implementation.

- Industry and other stakeholders should coordinate efforts to educate researchers and other potential Customers of nucleic acids of all nucleic acid procurement requirements for federal fundees.
- Institutions should support the research community in understanding Provider self-attestation and in purchasing nucleic acids from attesting Providers.

Recommendations

- OSTP and/or federal funding agencies should clarify how the OSTP Framework applies to Customers with mixed funding or with awards granted prior to implementation of the Framework (6 months).
- Federal funding agencies that implement the OSTP Framework should outline consequences for awardees of federal grants who are out of compliance (6 months).

References

1. Office of The Director, National Institutes of Health. NOT-OD-25-012: Notification of NIH Requirements Regarding Procurement of Synthetic Nucleic Acids and Benchtop Nucleic Acid Synthesis Equipment. *National Institute of Health (NIH).* 2024. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-012.html
2. Understanding and Implementing Nucleic Acid Synthesis Screening Policies in the US. *Gene Synthesis Screening Information Hub.* Accessed January 24, 2025. https://genesynthesisscreening.centerforhealthsecurity.org/

Conclusion

Affordable and accessible nucleic acid synthesis is a foundational life sciences capability that is enabling researchers to build biological solutions to the world's greatest challenges in health and medicine, food and agriculture, affordable energy, and climate and sustainability. The production and use of synthetic nucleic acids must be coupled with a cognizance of the dual use potential of some sequences and a commitment to developing and implementing practices that safeguard the technology and its use, without needlessly hindering progress.

Nucleic acid synthesis screening is an important safeguarding measure that can slow or stymie nefarious activity. In recent years, considerable public and private resources have been dedicated to both increasing adoption of basic nucleic acid synthesis screening practices and to advancing screening capabilities. The impact of these efforts on screening adoption is unclear, as there has never before been an incentive or codified mechanism for evaluating or assessing screening adoption and practices over time (e.g. via self-attestation of conformity). The release of the OSTP Framework and funding requirements for recipients of federally-funded researchers, for the first time, introduces an immediate economic incentive for screening. However, it also necessitates that clear standards are articulated, such that a Provider can be (self-)assessed for compliance to those standards. The OSTP Framework directs Providers to implement six actions in order to comply. Standards for some of those actions may be more straightforward to implement than others. For example, one action is to retain records of purchase orders, which aligns with common business practice. Specific information to record should become more standardized through adoption of the NIST Standard Guide. Another action is to implement cyber- and information security practices. NIST has several documents detailing how to best assess vulnerabilities and ensure cybersecurity. Here, we further recommend the development of a Cybersecurity Framework "Community Profile" for Providers.

Other actions required for adherence to the OSTP Framework, such as customer and sequence screening, are more challenging to adopt, disseminate, and implement. Significant progress was made through EBRC workshops in considering how the nucleic acid synthesis stakeholder community can move toward a sequence of concern paradigm that incorporates more sequence information than its taxonomy of origin. Consistent effort will be needed to build on the efforts and ideas of several individuals and groups as we collectively embrace this shift. Furthermore, test sets to support attestation and benchmarking will need to be further developed and administered to support consistent, quality screening and identify areas of ambiguity in screening. Ideally, in the future, sequences will be stratified by risk, and matrixed with Customer identity and legitimacy attributes to bring more nuance and decision-making support into challenging and currently subjective elements of Provider screening.

As nucleic acid synthesis capabilities continue to advance and spread around the world in tandem with converging technologies such as artificial intelligence and machine learning-assisted biodesign, it is crucial that stakeholders in the United States and internationally remain committed to developing resources and supporting nucleic acid synthesis Providers in the implementation of robust, cost-effective screening. Moving forward, efforts should also be made to work with international partners to identify and uphold best screening practices, overcoming barriers to screening together. Countries or regions with burgeoning bioeconomies must be supported and included so that screening practices and safeguards can be built into both nucleic acid procurement and into any current or future emerging synthesis capabilities.

Annex I: Virtual Workshop Agendas

EBRC

EBRC Engineering Biology Research Consortium

Enabling Quality, Measurable Synthetic DNA Sequence Screening

Virtual Workshop #1: Objectives and Challenges
Agenda

April 9, 2024
10 am - 12 pm PT | 1 pm - 3 pm ET
Join via Zoom

1:00 PM ET/ 10:00 AM PT	**Welcome and Introduction** *Becky Mackelprang*, EBRC
1:05 PM ET / 10:05 AM PT	**Project background, aims, and approach** USG efforts to support and enable screening *Mariam Lekveishvili*, HHS ASPR NIST's Role and the Executive Order on AI *Sheng Lin-Gibson*, NIST Project Aims and Approach *Becky Mackelprang*, EBRC
1:50 PM ET / 10:50 AM PT	**SOC Database(s): Context, challenges, and opportunities** *Kevin Flyangolts*, Aclid Discussant: *Lenny Foner*, SecureDNA
2:10 PM ET/ 11:10 AM PT	**Test Dataset(s): Context, challenges, and opportunities** *Jake Beal*, RTX BBN Discussant: *Scott Jackson*, NIST
2:30 PM ET / 11:30 AM PT	**Breakout Rooms** Room A: Needs for building an effective SOC database (Room A Google Doc) *Facilitator:* India Hook-Barnard, EBRC Room B: Needs for building an effective test dataset (Room B Google Doc) *Facilitator:* Becky Mackelprang, EBRC
2:45 PM ET / 11:45 AM PT	**Return and Report** *India Hook-Barnard*, EBRC
2:55 PM ET / 11:55 AM PT	**Concluding thoughts, next steps, and further opportunity to engage** *Becky Mackelprang*, EBRC

Workshop Objectives:

- Communicate project background, objectives, context, and approach.
- Identify and discuss considerations for building a Sequence of Concern database, including currently used databases, curation, and security and access.
- Identify and discuss considerations for developing test dataset(s) for measuring DNA screening tool performance.
- Elucidate topics for future workshops.

EBRC

EBRC Engineering Biology Research Consortium

Enabling Quality, Measurable Synthetic DNA Sequence Screening

Virtual Workshop #2: Sequence of Concern Databases—What's Regulated?
Agenda

May 2, 2024
12pm - 2pm PT | 3pm - 5pm PT
Join via Zoom

3:00 PM ET/ 12:00 PM PT	**Welcome and Introduction to Workshop #2** *Becky Mackelprang*, EBRC
3:15 PM ET / 12:15 PM PT	**Export Control** *Kimberly Orr, Bureau of Industry and Security at U.S. Department of Commerce*
3:25 PM ET / 12:20 PM PT	**Regulations and Remaining Questions** *Craig Bartling*, Battelle
3:45 PM ET / 12:45 PM PT	**Breakout Discussions: Screening for sequences from regulated agents** Topic A: Interpreting regulation: Determining which sequences from regulated agents are regulated/controlled *Facilitator: India Hook-Barnard*, EBRC Topic B: Screening practices for identifying genetic elements / nucleic acids subject to regulation *Facilitator: Becky Mackelprang,* EBRC
4:30 PM ET / 1:30 PM PT	**Return and Report** What did we get clarity on and what did we not? What are outstanding questions?
4:40 PM ET/ 1:40 PM PT	**Emerging Capabilities - Determining a Threat Model** *Jens Berlips*, SecureDNA
4:50 PM ET / 1:50 PM PT	**Concluding thoughts, next steps, and further opportunity to engage** *Becky Mackelprang*, EBRC
5:00 PM ET / 2:00 PM PT	**Adjourn**

EBRC

EBRC Engineering Biology Research Consortium

Enabling Quality, Measurable Synthetic DNA Sequence Screening

Virtual Workshop #3: Functions and parameters of test data sets

Agenda

May 31, 2024

10am - 12pm PT | 1pm - 3pm ET

Join via Zoom

1:00 PM ET/ 10:00 AM PT	**Welcome; Reflections on Workshops #1 & 2, Introduction to Workshop #3** *Becky Mackelprang*, EBRC
1:20 PM ET / 10:20 AM PT	**Discussion:** Parameters of Conformity Assessment and Benchmarking Data Sets
2:25 PM ET / 11:25 AM PT	**Conformity Assessment and Self-Attestation for October 2024:** *Sheng Lin-Gibson*, NIST | Draft Self-Attestation Template *Scott Jackson*, NIST | Process for NIST Test Set
2:55 PM ET / 11:55 AM PT	**Concluding thoughts, next steps, and further opportunity to engage** *Becky Mackelprang*, EBRC
3:00 PM ET / 12:00 PM PT	**Adjourn**

EBRC

EBRC Engineering Biology Research Consortium

Enabling Quality, Measurable Synthetic DNA Sequence Screening

Virtual Workshop #4: Sequences of Concern

Agenda

June 27, 2024
10am - 12pm PT | 1pm - 3pm ET
Join via Zoom

1:00 PM ET/ 10:00 AM PT	**Welcome and Introduction to Workshop #4** *Becky Mackelprang*, EBRC
1:10 PM ET/ 10:10 AM PT	**Sequences of Concern - USG Perspective** *Kathleen Danskin,* ASPR | Department of Health and Human Services
1:20 PM ET/ 10:20 AM PT	**Sequences of Concern - Industry Perspective** *Jason Middleton*, Battelle
1:30 PM ET/ 10:30 AM PT	**Evaluating the security relevance of bacterial and fungal sequences by whether possession would expand access to a regulated capability** *Kevin Esvelt*, MIT
1:40 PM ET/ 10:40 AM PT	**Functions of Concern** *Gene Godbold*, Signature Science
1:55 PM ET/ 10:55 AM PT	**Discussion: Sequences of Concern** Axes for adjudicating concern Gradations within those axes
2:55 PM ET/ 11:55 AM PT	**Concluding thoughts, next steps, and further opportunity to engage** *Becky Mackelprang*, EBRC
3:00 PM ET/ 12:00 PM PT	**Adjourn**

EBRC

EBRC Engineering Biology Research Consortium

Enabling Quality, Measurable Synthetic DNA Sequence Screening

Virtual Workshop #5: Customer Screening
Agenda

July 25, 2024
11am - 1pm PT | 2pm - 4pm ET
Join via Zoom

2:00 PM ET/ 11:00 AM PT	**Welcome and Introduction to Workshop #5** *Becky Mackelprang*, EBRC
2:10 PM ET/ 11:10 AM PT	**Developing a Customer Screening Framework for the Life Sciences** *Sarah Carter,* Science Policy Consulting
2:20 PM ET / 11:20 AM PT	**Integrated Customer and Sequence Screening** *Kevin Flyangolts*, Aclid
2:30 PM ET/ 11:30 AM PT	**SecureDNA's Customer Screening Approach** *Jens Berlips*, SecureDNA
2:40 PM ET/ 11:40 AM PT	**Discussion: Customer Screening Best Practices** Standardizing customer interactions Demonstrating legitimacy
3:15 PM ET/ 12:15 PM PT	**Self-Attestation of Customer Screening** *Sheng Lin-Gibson*, NIST
3:25 PM ET/ 12:25 PM PT	**Discussion Continued**
3:55 PM ET/ 12:55 PM PT	**Concluding thoughts, next steps, and further opportunity to engage** *Becky Mackelprang*, EBRC
4:00 PM ET/ 1:00 PM PT	**Adjourn**

EBRC

EBRC Engineering Biology Research Consortium

Enabling Quality, Measurable Synthetic DNA Sequence Screening

Virtual Workshop #6: Best Practices and Outstanding Questions for Implementation

Agenda

August 14, 2024
10am - 12pm PT | 1pm - 3pm ET
Join via Zoom

1:00 PM ET / 10:00 AM PT	**Welcome and Introduction to Workshop #6** *Becky Mackelprang*, EBRC
1:05 PM ET / 10:05 AM PT	**Discussion** Best Practices and Outstanding Questions for Oct 2024 Implementation of OSTP FW
2:30 PM ET / 11:30 AM PT	**Cybersecurity Supply Chain Management** *Laura Calloway*, NIST
2:45 PM ET/ 11:45 AM PT	**Digital ID Management for Customer Screening** *Ryan Galluzo*, NIST
3:00 PM ET/ 12:00 PM PT	**Adjourn**

Annex II: In-Person Workshop Agenda

EBRC Engineering Biology Research Consortium

Enabling Quality, Measurable DNA Sequence Screening

EBRC / NIST Workshop

Hilton Garden Inn
7301 Waverly St, Bethesda, MD 20814
Chevy Chase / Montgomery Rooms

September 10-11, 2024

At times over the coming two days, we will collect your ideas and input on this Google Doc. Please keep this link handy!

If you can't see the slides, you can follow along here

Day 1: Tuesday September 10, 2024	
9:00 AM ET	**WELCOME & INTRODUCTION** Becky Mackelprang, *EBRC*
9:20 AM	**Introduction and adherence to OSTP Framework in October 2024** Daniel Gastfriend, *Director for Biodefense and Pandemic Preparedness, National Security Council*
9:35 AM	**Panel: Questions, challenges, and opportunities for the 2024 implementation of the OSTP Framework** *This panel will feature different stakeholders and highlight the challenges and opportunities for implementing the OSTP Framework.* *Moderated by* Becky Mackelprang, *EBRC* *Panelists:* James Diggans, *Head of Biosecurity, Twist Biosciences* Kevin Flyangolts, *CEO, Aclid* Jean Peccoud, *Professor, Colorado State University* Melissa Hopkins, *Health Security Policy Analyst, Johns Hopkins Center for Health Security* Wendy Hall, *Senior Advisor to the DAS, Department of Homeland Security* Daniel Gastfriend, *Director for Biodefense and Pandemic Preparedness, National Security Council*

10:20 AM	**Break**
10:50 AM	**Toward consensus: Statements and recommendations** *Identifying areas of consensus and where further discussion is needed.* Becky Mackelprang*, EBRC* Link to consensus statements and recommendations
12:00 PM	**Lunch**
1:00 PM	**Customer Screening: Standardizing customer information collection** *See OSTP Framework Action 3.* *A sample of customer questions and a Provider decision tree will be workshopped for ascertaining customer legitimacy both at the time a SOC is ordered and during follow-up.* *Speakers / Discussion Facilitators:* Tessa Alexanian*, Tech Lead: Common Mechanism, IBBIS* Sarah Carter*, Science Policy Consulting LLC*
2:10 PM	**Education, outreach, and attestation** *See OSTP Framework Action 1.* *Which stakeholder groups need to be aware of new policies, but are not? Workshop informational 1-pagers for these stakeholder groups and consider options for distribution.* *Speaker:* Melissa Hopkins*, Health Security Policy Analyst, Johns Hopkins Center for Health Security* Email address for Questions for USG: syndnaguidance@hhs.gov Website Customer Form Provider Form *Discussion facilitated by* Sebastian Rivera, *Science Policy Postdoc, EBRC*
3:10 PM	**Break**
3:40 PM	**Assessing Screening System Performance** *See OSTP Framework Action 2.* *Update on test set for screening performance in Oct* 2024 *and the development and maintenance of Conformity and Benchmarking Test Sets into the future.* *Speakers:* Sam Forry, *Research Scientist, NIST* Jacob Beal, *Engineering Fellow, Raytheon BBN* *Discussion facilitated by* Becky Mackelprang, *Director for Security Programs, EBRC*

5:00 PM ET	**ADJOURN**

DAY 2: Wednesday September 11, 2024	
9:00 AM	**DAY 2 WELCOME** Becky Mackelprang, *EBRC*
9:10 AM	**A Paradigm Shift in our Approach to "Sequence of Concern?" From 2024 toward function-based approaches** *See OSTP Framework Action 2.* *The challenges of list-based approaches to identifying SOCs are well understood. How ready are we for a function-based approach to sequences of concern? What else needs to happen?* *Speakers:* James Diggans, *Head of Biosecurity, Twist Biosciences* Craig Bartling, *Senior Biological Data Scientist, Battelle* *Discussion facilitated by* Becky Mackelprang, *Director for Security Programs, EBRC*
10:10 AM	**Break**
10:40 AM	**AI and Nucleic Acid Sequence Screening** *As biodesign tools and capabilities advance, how can nucleic acid synthesis screening not just keep up, but stay ahead? Are screening systems robust to AI-generated novel sequences?* *Speakers:* Jacob Beal, *Engineering Fellow, Raytheon BBN* Craig Bartling, *Senior Biological Data Scientist, Battelle* Stephanie Guerra, *Senior Advisor, U.S. AI Safety Institute/NIST*
11:40 AM	**Cybersecurity and Information Security** *See OSTP Framework Action 6.* *Securing Sequence of Concern Databases, supply chain risk management, cybersecurity, and customer identity and IP protection.* *Speakers / Facilitators:* Laura Calloway, *IT Specialist, NIST* Justin Wagner, *Computer Scientist, NIST*
12:40 PM	**Lunch**

1:40 PM	**Follow-Up Screening, Reporting, and Decision-Making Support** *See OSTP Framework Action 4.* *When a SOC is flagged, how do Providers decide if customer contact is required? In which situations should Providers report an order to Law Enforcement, and in what form should that reporting occur?* *Speaker:* William So*, Program Manager - National and Biological Security Policy, FBI* --- IBBIS Screening Exercise Tessa Alexanian*, Technical Lead, International Biosecurity & Biosafety Initiative for Science*
3:00 PM	**Break**
3:20 PM	**Record retention, formatting, and synthesis** *See OSTP Framework Action 5.* *In what format should records be kept? What information needs to be recorded and retained?* *Speaker / Facilitator:* Steven Fairchild*, Principal Biotechnologist, The MITRE Corporation*
4:10 PM	**International Nucleic Acid Screening** *How can best practices expand beyond the United States? What will be challenging about internationalizing best practices?*
4:50 PM	**FINAL THOUGHTS & WRAP-UP**
5:00 PM	**ADJOURN**

Annex III: NIST Draft Standard Guide for Providers

Standard Guide for Providers in support of self attestation to the Framework for Nucleic Acid Synthesis Screening

Version date: Jan 22, 2015

NOTE: To be posted by EBRC and tested by IGSC

This sample template serves as a tool to support harmonized self-attestation documentation by Providers[1] under the National Science and Technology Council's "Framework for Nucleic Acid Synthesis Screening" (April 2024) (the "Framework"). These self-attestations are designed to allow customers[2] and end users[3] of synthetic nucleic acids to select a Provider that is adherent to the Framework.

The sample template is based on ISO/IEC 17050-1:2004 *Conformity Assessment – Supplier's declaration of conformity Part 1: General Requirement,*[4] an international standard that specifies general requirements for a supplier's self-attestation.

This document was developed through collaboration with the Engineering Biology Research Consortium (EBRC)[5] and International Gene Synthesis Consortium (IGSC),[6] among others.

NOTE: Manufacturer[7] should see *Internal Checklist for Manufacturers* in their self attestation to the Framework.

[1] The Framework defines a "Provider" as "An entity that synthesizes and distributes synthetic nucleic acids. Providers may provide nucleic acids to a customer or third-party vendor. A Provider is understood to be synthesizing and distributing nucleic acids as a transactional service, rather than as a research scientist collaborating with a colleague."
[2] The Framework defines "Customer" as "The individual or entity (such as an institution) that orders or requests synthetic nucleic acids from a Provider, or that purchases nucleic acid synthesis equipment from a Manufacturer."
[3] The term "end user" refers to the individual or persons design or executing research using the synthetic nucleic acids
[4] ISO/IEC 17050 specifies requirements applicable when the individual or organization responsible for fulfilment of specified requirements (supplier) provides a declaration that a product (including service), process, management system, person or body is in conformity with specified requirements, which can include normative documents such as standards, guides, technical specifications, laws and regulations.
[5] https://ebrc.org/
[6] https://genesynthesisconsortium.org
[7] The Framework defines a "Manufacturer" as "An entity that produces and distributes benchtop equipment for synthesizing nucleic acids. Manufacturers may provide equipment to a customer or third-party vendor."

Template

The Framework calls for federal funding agencies, as appropriate and consistent with applicable law, to ensure that synthetic nucleic acids procured using federal funds are sourced from Providers that are in compliance with the Framework via self-attestation.

This document provides an overview of the contents of an attestation that Providers can make to assert compliance with the processes and safeguards reflected in the Framework.

This template provides a harmonized approach and encourages uniform documentation towards more robust sequence screening, customer identification verification, and customer legitimacy determination. Further, common data collection fields facilitate record retention and data aggregation across providers.

Providers are not expected to share data collected with the general public. Information collected may be reviewed by third party (e.g., conformity assessment body) with approval of the Provider or submitted to law enforcement.

This document is intended to be further developed as an industry standard in support of conformity assessment.

General Declaration Statements:

- **Declarations Statement 1**: Screen purchase orders for synthetic nucleic acids to identify Sequences of Concern (SOCs).[8]
- **Declarations Statement 2**: Screen customers submitting purchase orders of synthetic nucleic acids with SOCs to verify legitimacy.
- **Declarations Statement 3**: Report potentially illegitimate purchase orders of synthetic nucleic acids involving SOCs.
- **Declarations Statement 4**: Retain records relating to purchase orders for synthetic nucleic acids for at least three years.
- **Declarations Statement 5**: Take steps to ensure cybersecurity and information security.

Questions with a star (*) are required fields

[8] The Framework defines a Sequence of Concern as, at the time of its issuance "a nucleotide sequence or its corresponding amino acid sequence that is a Best Match to a sequence of federally regulated agents (i.e., the Biological Select Agents and Toxins List (BSAT), or the Commerce Control List (CCL)), except when the sequence is also found in an unregulated organism or toxin. As of and after October 13, 2026, this definition will include sequences known to contribute to pathogenicity or toxicity, even when not derived from or encoding regulated biological agents[.]".

Part I: Organization (Provider) information, baseline sequence screening, and conformity attestation (one time/annual update)

The following supports **Declaration Statements 1 and 4.**

The use of a third-party screening tool is highly encouraged. Providers who wish to use *in house* sequence screening tools should develop and document processes and procedures to ensure that screening tools are kept up-to-date with respect to emerging threats.

1. Organization name*	
2. Unique Attestation Identifier* *Identifiers are not currently in use, but may be useful to pursue moving forward*	
3. Unique Entity Identifier (UEI)[9]	
4. Tax ID Number (EIN)[10]	
5. Address*	
6. Type of NA provider (check all that apply): Note: see footnote 1 for definitions	☐ Commercial Nucleic Acid sequence provider ☐ Manufacturer of Nucleic Acid synthesis equipment ☐ Third-party vendor ☐ Biofoundry ☐ Cloud Lab ☐ Core Facility / Academic Core Facility ☐ Contract Research Organization (CRO) ☐ Other (please specify): _____
7. Sequence screening tool in use*: (check all that apply) NOTE: additional considerations to be addressed by the stakeholders/community 1) Mechanism to be developed to periodically update the list and	Commercial Third-party Screening tools: ☐ Aclid ☐ Battelle ThreatSeq / UltraSEQ ☐ IBBIS Common Mechanism ☐ RTX BBN FAST-NA Scanner ☐ SecureDNA ☐ Other

[9] A UEI is a government-provided number, like a tax ID number, that's used to identify businesses eligible for federal grants, awards and contracts. Within the U.S., the UEI will be requested in, and assigned by, the System for Award Management (SAM.gov).

[10] An EIN is a unique nine-digit number that identifies the business for tax purposes. Within U.S., EIN is obtained from the IRS.

version of third party screening tools (e.g. provide link to most up-to-date of third party screening tools)	If other, version and release date of the Third-party screening tool: _____ In-house screening tools: name of the tool, tool description and database _____
8. Sequence screening baseline testing	Date of last baseline sequence screening test pass ____ Test set version _____ Baseline screening test administrator (e.g., IBBIS) _____ Link/identifier to baseline sequence screening test results _____
9. Date of last self attestation to 5 Declaration Statements*	
10. URL of the last self attestation reference above	
11. Scope of operations covered by self attestation (geographical limitations, e.g., for companies synthesizing sequences at multiple sites, is the sequence screening centralized or conducted differently at each site)*	
12. Name and title of person responsible for self attestation*	

Part II: Template for harmonized order information (with each order)

The following information will be requested from customers to support **Declaration Statements 1, 2, and 4**, including verifying customer identity, screening sequences, and determining customer legitimacy, if needed.

1. Customer name*	
2. Customer affiliation*	
3. Customer address*	
4. Customer phone*	

5. Customer email*	
6. **Place holder** for customer identify verification mechanisms	
7. Sequences ordered* (compatible with FASTA file format)	
8. Is the order known to contain nucleic acid sequence(s) encoding genes unique to regulated organisms (i.e., the Biological Select Agents and Toxins List (BSAT), or the Commerce Control List (CCL)) that are associated with toxicity or pathogenicity?*	☐ No ☐ Yes ☐ Unknown The answer to this question should be YES, if evidence provided by the recipient's Responsible Official that the Recipients is registered with the Federal Select Agent Program (FSAP) or Statement by Ultimate Consignee and Purchaser (i.e., completed BIS-711 form):
9. Is the order known to contain nucleic acid sequence(s) encoding functional genes that may endow enhanced pathogenicity or toxicity to potentially threaten human and non-human health?* Note: In the U.S. this question supports compliance to DURC-PEPP policy [11]	☐ No ☐ Yes ☐ Unknown
If the answer is 'yes' or 'unknown' to questions 8 or 9, please provide the following as appropriate – whereas some of these types of information may be sufficient solely to establish legitimacy, others may establish legitimacy in combination:	
10. End User name(s)	
11. End User shipping address(es)	

[11] https://www.whitehouse.gov/wp-content/uploads/2024/05/USG-DURC-PEPP-Implementation-Guidance.pdf

12. End User phone number(s)	
13. End User email(s)	
14. End User ORCID(s)	
15. Grant number(s)	
16. Organization business licenses (e.g. Unique Entity Identifier (UEI))	
17. Category of intended use for sequence order	☐ General R&D (gene will be expressed) ☐ General R&D (gene will not be expressed) ☐ Diagnostic test development ☐ Therapeutic development ☐ Other Description If other, name of the purpose of intend use _____
18. Description of intended use for sequence order	
19. Name of biosafety/biosecurity officer	
20. Address of biosafety/biosecurity officer	
21. Email of biosafety/biosecurity officer	
22. Phone number of biosafety/biosecurity officer	
23. Do you have documentation of internal review and approval of the research?	☐ Yes ☐ No
24. Biosafety level of the lab where the work with the requested genes will be conducted	☐ BSL 1 ☐ BSL 2 ☐ BSL 3 ☐ BSL 4

Part III: Customer Identity verification (during account set up or with the placement of the first order)

The following information will be recorded and saved to support **Declaration Statement 4**.

Providers should document requirements associated with regional regulation, including Restricted Party Screening (RPS). A third party tool can be used for RPS.

The IGSC requires all customers to be screened against OFAC's SDN List, the Department of State's Debarred List, the BIS Denied Persons, Entity, and Unverified lists, and the HADDEX list.

1. Was customer identity verified?*	☐ Yes ☐ No
2. Is the customer prohibited from commercial transactions under regional regulations?*	☐ Yes ☐ No
3. Third party RPS tool in use:	

Part IV: Sequence screening and customer legitimacy (completed/saved for each ordered sequence)

The following information will be collected and saved to support **Declaration Statements 2 and 4**.

1. Generate unique order identifier linking to the information provided in Part II…	
2. Individual sequence ordered (from list in Part II, question 7)	
3. Sequence screening result	☐ Flag ☐ No flag
4. If Sequence was Flagged, what additional customer interaction was attempted?	
5. If Sequence was Flagged, how was customer legitimacy established?	
6. Was the order fulfilled?	
7. Date of order fulfillment?	

Part V: Report potentially illegitimate purchase orders

The following supports **Declarations Statement 3**, report potentially illegitimate purchases. The list below captures information in addition those captured in Part II, which are generally submitted to law enforcement organizations.

1. Flag sequence(s)*	
2. Further customer screening interaction(s)*	
3. Rationale for decisions about the legitimacy of customer and/or order *	
4. Reporting to authorities*	☐ U.S. FBI Field Office ☐ U.S. DoC Bureau of Industry and Security ☐ U.S. DHS CISA ☐ Other: _____
5. Reporting Date*	
6. Additional interactions with authorities	
7. Outcome of interactions with authorities	

Part VI: Ensure cybersecurity and information security (in support of Declaration Statement 5)

Providers may consider the following tools in the development of cybersecurity and information security best practices.

Larger organizations with sufficient resources should consider following *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

Smaller organizations should consider the following Quick Start Guides:
CSF 2.0 Quick Start Guide for Small Businesses to Review Overall Organization Cybersecurity Risk Management
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf

CSF 2.0 Quick Start Guide to Assess Organization Cybersecurity Supply Chain Risk Management Strategies
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1305.ipd.pdf

Part VII: Record Keeping (in support of Declaration Statement 4)

All information collected using Part I-VI, including updated internal screening/tested methods and results, should be retained for at least 3 years.

Annex Sections

The section below provides recommendations for harmonized sequence screening process